# Programmabeleid voor ontwikkelaars

*(vanaf 6 maart 2024, tenzij anders aangegeven)*

### Samen bouwen aan 's werelds meest betrouwbare bron voor apps en games

Uw innovatie is de drijvende kracht achter ons gedeelde succes, maar daar hoort wel een verantwoordelijkheid bij. Dit Programmabeleid voor ontwikkelaars, samen met de Distributieovereenkomst voor ontwikkelaars, garandeert dat we via Google Play de meest innovatieve en vertrouwde apps ter wereld blijven leveren aan meer dan een miljard mensen. U kunt ons beleid hieronder bekijken.

## Beperkte content

Elke dag gebruiken mensen over de hele wereld Google Play om toegang tot apps en games te krijgen. Voordat u een app indient, moet u zich afvragen of uw app geschikt is voor Google Play en voldoet aan de lokale wetgeving.

### In gevaar brengen van kinderen

Apps die gebruikers geen verbod opleggen voor het maken, uploaden of distribueren van content die de uitbuiting of het misbruik van kinderen faciliteert, worden onmiddellijk verwijderd van Google Play. Dit omvat alle materiaal met daarop seksueel misbruik van kinderen. Klik op **Misbruik melden** om content in een Google-product te melden waarin een kind misschien wordt uitgebuit. Als u dergelijke content ergens anders op internet tegenkomt, neemt u rechtstreeks contact op met de aangewezen instantie in uw land .

We verbieden het gebruik van apps om kinderen in gevaar te brengen. Dit omvat, maar is niet beperkt tot, het gebruik van apps om roofdiergedrag richting kinderen te bevorderen, zoals:

- Ongepaste interactie met een kind (zoals betasten of strelen).
- Kinderlokken (bijvoorbeeld online vriendschap sluiten met een kind om online of offline seksueel contact mogelijk te maken en/of seksuele beelden uitwisselen met dat kind).
- Seksualisering van een minderjarige (bijvoorbeeld afbeeldingen die seksueel misbruik van kinderen laten zien, aanmoedigen of promoten of kinderen tonen op een manier die kan leiden tot seksuele uitbuiting van kinderen).
- 'Sextortion' (bijvoorbeeld een kind bedreigen of chanteren door echte of vermeende toegang tot intieme afbeeldingen van het kind te gebruiken).
- Kinderhandel (bijvoorbeeld een kind aanbieden of lokken voor commerciële seksuele uitbuiting).

Als wij content met materiaal met daarop seksueel misbruik van kinderen aantreffen, nemen we passende maatregelen. Zo kunnen we melding maken bij instanties voor kindermisbruik (zoals het Amerikaanse National Center for Missing & Exploited Children). Als u vermoedt dat een kind in gevaar verkeert of het slachtoffer is van misbruik, uitbuiting of kinderhandel, neem dan contact op met de plaatselijke politie en met een hier vermelde organisatie die zich inzet voor de veiligheid van kinderen.

Bovendien zijn geen apps toegestaan die aantrekkelijk zijn voor kinderen maar thema's voor volwassenen bevatten, inclusief maar niet beperkt tot:

- Apps met overmatig geweld, bloed en bloedvergieten.
- Apps die schadelijke en gevaarlijke activiteiten tonen of aanmoedigen.

We staan ook geen apps toe die een negatief lichaams- of zelfbeeld promoten, waaronder apps die voor amusementsdoeleinden plastische chirurgie, afvallen en andere cosmetische aanpassingen van

de fysieke verschijning van een persoon tonen.

## Ongepaste content

We hebben normen opgesteld die content definiëren en verbieden die schadelijk of ongepast is voor onze gebruikers om ervoor te zorgen dat Google Play een veilig en respectvol platform blijft.

## Seksuele content en grof taalgebruik

We staan geen apps toe die seksuele content of grof taalgebruik bevatten of promoten, waaronder pornografie, of content en services die zijn bedoeld voor seksuele bevrediging. We staan geen apps of app-content toe die een seksuele handeling in ruil voor een vergoeding lijken te promoten of te vragen. We staan geen apps toe die content bevatten of promoten die verband houdt met seksueel roofdiergedrag of die seksuele content distribueren zonder wederzijds goedvinden. Content met naakt kan worden toegestaan als deze primair bedoeld is voor educatieve, informatieve, wetenschappelijke of artistieke doeleinden en als het gebruik van deze beelden niet ongegrond is.

Als een app content bevat die dit beleid schendt maar die als gepast wordt beschouwd in een bepaalde regio, is de app mogelijk beschikbaar voor gebruikers in die regio maar niet voor gebruikers in andere regio's.

We hebben normen opgesteld die content definiëren en verbieden die schadelijk of ongepast is voor onze gebruikers om ervoor te zorgen dat Google Play een veilig en respectvol platform blijft.

- Afbeeldingen van seksuele naakt of seksueel suggestieve poses waarin een persoon naakt is, vervaagd is of minimale kleding aan heeft en/of als deze kleding in een passende openbare context niet acceptabel zou zijn.
- Afbeeldingen, animaties of illustraties van seksuele handelingen of seksueel suggestieve poses of de seksuele weergave van lichaamsdelen.
- Content waarin seksuele hulpmiddelen, seksgidsen, illegale seksuele thema's en fetisjen worden afgebeeld of content die functioneel als zodanig kan worden aangemerkt.
- Obscene of grove content, inclusief maar niet beperkt tot content die grof taalgebruik, scheldwoorden, expliciete teksten, seksuele zoekwoorden of zoekwoorden voor volwassenen bevat in de winkelvermelding of in de app.
- Content die bestialiteit afbeeldt, beschrijft of aanmoedigt.
- Apps die seksgerelateerd entertainment, escortservices of andere services promoten die kunnen worden opgevat als het aanbieden van of vragen naar seksuele handelingen tegen een vergoeding, inclusief maar niet beperkt tot daten tegen vergoeding of seksuele verhoudingen waarbij van één deelnemer wordt verwacht dat deze een andere deelnemer geld, cadeaus of financiële steun biedt (zoals 'sugar dating').
- Apps die mensen denigreren of objectiveren, zoals apps die beweren mensen uit te kleden of door hun kleding heen te kijken, ook als ze zijn gelabeld als apps voor pranks of entertainment.
- Content of gedrag dat personen op een seksuele manier probeert te bedreigen of uit te buiten, zoals creepshots, een verborgen camera, seksuele content zonder wederzijds goedvinden die via een deepfake of soortgelijke technologie is gemaakt, of content met misbruik.

## Aanzetten tot haat

We staan geen apps toe die geweld of haat promoten tegen personen of groepen op basis van ras, etnische afkomst, religie, beperkingen, leeftijd, nationaliteit, veteranenstatus, seksuele geaardheid, gender, genderidentiteit, kaste, immigratiestatus of elk ander kenmerk dat wordt gekoppeld aan systemische discriminatie of marginalisatie.

Apps die content voor educatieve, wetenschappelijke, artistieke of documentairedoeleinden bevatten die betrekking heeft op nazi's, kunnen in bepaalde landen worden geblokkeerd in overeenstemming met de lokale wet- en regelgeving.

We hebben normen opgesteld die content definiëren en verbieden die schadelijk of ongepast is voor onze gebruikers om ervoor te zorgen dat Google Play een veilig en respectvol platform blijft.

- Content of taalgebruik waarin wordt beweerd dat een beschermde groep onmenselijk of minderwaardig is of het verdient om te worden gehaat.
- Apps met haatdragende uitdrukkingen, stereotypen of theorieën dat een beschermde groep negatieve kenmerken heeft (zoals kwaadaardig, corrupt, enzovoort) of die impliciet of expliciet stellen dat de groep een bedreiging vormt.
- Content of uitspraken om anderen te doen geloven dat mensen moeten worden gehaat of gediscrimineerd omdat ze lid zijn van een beschermde groep.
- Content die haatsymbolen, zoals vlaggen, symbolen, insignes, attributen of gedrag in verband met haatgroepen promoot.

## Geweld

We staan geen apps toe die zinloos geweld of andere gevaarlijke activiteiten afbeelden of mogelijk maken. Apps die fictief geweld in de context van een game weergeven, zoals tekenfilms, jagen of vissen, zijn over het algemeen toegestaan.

We hebben normen opgesteld die content definiëren en verbieden die schadelijk of ongepast is voor onze gebruikers om ervoor te zorgen dat Google Play een veilig en respectvol platform blijft.

- Grafische afbeeldingen of beschrijvingen van realistisch geweld of gewelddadige bedreigingen tegen een persoon of dier.
- Apps die zelfbeschadiging, zelfmoord, eetstoornissen, wurgspellen of andere handelingen promoten waarbij ernstig letsel of de dood kan optreden.

**Terroristische content**

Het is terroristische organisaties niet toegestaan apps te publiceren op Google Play voor welk doel dan ook, inclusief werving.

We staan ook geen apps toe met content over terrorisme waarin bijvoorbeeld tot terroristische acties of geweld wordt aangezet of waarin terroristische aanslagen worden gevierd. Als u aan terrorisme gerelateerde content post voor educatieve, wetenschappelijke of artistieke doeleinden, of in de context van een documentaire, moet u voldoende informatie bieden, zodat gebruikers de EIWA-context begrijpen.

**Gevaarlijke organisaties en bewegingen**

We staan bewegingen of organisaties die betrokken zijn geweest bij, zich hebben voorbereid op of verantwoordelijkheid hebben opgeëist voor gewelddadige handelingen tegen burgers, niet toe apps op Google Play te publiceren voor welk doel dan ook, waaronder werving.

We staan geen apps toe met content die verband houdt met het plannen, voorbereiden of verheerlijken van geweld tegen burgers. Als uw app dergelijke content bevat voor een EIWA-doel, moet u de relevante EIWA-context bieden voor die content.

## Gevoelige gebeurtenissen

We staan geen apps toe die profiteren van of ongevoeligheid tonen ten opzichte van een gevoelige gebeurtenis met aanzienlijke sociale, culturele of politieke gevolgen, zoals noodsituaties, natuurrampen, bedreigingen van de volksgezondheid, conflicten, sterfgevallen of andere tragische gebeurtenissen. Apps met content over een gevoelige gebeurtenis zijn over het algemeen toegestaan als die content een educatieve, wetenschappelijke, artistieke of documentaire waarde heeft of gebruikers wil wijzen op of bewust wil maken van de gevoelige gebeurtenis.

We hebben normen opgesteld die content definiëren en verbieden die schadelijk of ongepast is voor onze gebruikers om ervoor te zorgen dat Google Play een veilig en respectvol platform blijft.

- Gebrek aan gevoeligheid over de dood van een echt persoon of groep mensen als gevolg van zelfmoord, overdosis, natuurlijke oorzaken, enzovoort.
- Ontkenning van het plaatsvinden van een goed gedocumenteerde, omvangrijke tragische gebeurtenis.
- Profiteren van een gevoelige gebeurtenis zonder waarneembare voordelen voor de slachtoffers.

## Pesten en intimidatie

We staan geen apps toe die bedreigingen, intimidatie of pesten bevatten of mogelijk maken.

We hebben normen opgesteld die content definiëren en verbieden die schadelijk of ongepast is voor onze gebruikers om ervoor te zorgen dat Google Play een veilig en respectvol platform blijft.

- Slachtoffers van internationale of religieuze conflicten kwetsen.
- Content die anderen probeert te exploiteren, zoals afpersing, chantage, enzovoort.
- Content posten om iemand publiekelijk te vernederen.
- De slachtoffers van een tragische gebeurtenis, of hun vrienden en familie, lastigvallen.

## Gevaarlijke producten

We staan geen apps toe die de verkoop van explosieven, vuurwapens, munitie of bepaalde accessoires voor vuurwapens mogelijk maken.

- Beperkte accessoires zijn onder meer die welke ervoor zorgen dat een vuurwapen gaat lijken op een automatisch vuurwapen of waarmee van een vuurwapen een automatisch vuurwapen kan worden gemaakt (zoals bump stocks, trekkers voor mitrailleurs, pallen voor aanvalsgeweren, ombouwkits) en magazijnen of riemen met meer dan 30 patronen.

We staan geen apps toe die instructies geven voor het vervaardigen van explosieven, vuurwapens, munitie, beperkte vuurwapenaccessoires of andere wapens. Dit omvat tevens instructies voor het ombouwen van een vuurwapen zodat het automatisch kan vuren of lijkt alsof het automatisch kan vuren.

## Marihuana

We staan geen apps toe die de verkoop van marihuana of marihuanaproducten mogelijk maken, ongeacht of marihuana legaal is of niet.

We hebben normen opgesteld die content definiëren en verbieden die schadelijk of ongepast is voor onze gebruikers om ervoor te zorgen dat Google Play een veilig en respectvol platform blijft.

- Gebruikers in staat stellen marihuana te bestellen met behulp van een winkelwagenfunctie in de app.
- Gebruikers helpen de levering of het ophalen van marihuana te regelen.
- De verkoop van producten met THC (tetrahydrocannabinol) mogelijk maken, waaronder producten als CBD-olie met THC.

## Tabak en alcohol

We staan geen apps toe die de verkoop van tabak (waaronder e-sigaretten en vape-pennen) mogelijk maken of het illegale of ongepaste gebruik van alcohol of tabak aanmoedigen.

**Aanvullende informatie**

- Het gebruik of de verkoop van alcohol of tabak aan minderjarigen afbeelden of aanmoedigen is niet toegestaan.

- Impliceren dat de consumptie van tabak iemands sociale, seksuele, professionele, intellectuele of atletische status kan verbeteren is niet toegestaan.
- Overmatig drankgebruik op positieve wijze afbeelden, waaronder een positief beeld van overmatig alcoholgebruik, comazuipen of drankwedstrijden, is niet toegestaan.
- Advertenties, promoties of prominente aanbevelingen van tabaksproducten (waaronder advertenties, banners, categorieën en links naar sites waarop tabak wordt verkocht) zijn niet toegestaan.
- In bepaalde regio's staan we misschien de beperkte verkoop van tabaksproducten toe in apps voor het bezorgen van eten/boodschappen en onder voorbehoud van leeftijdschecks (zoals een ID-controle bij bezorging).

---

## Financiële dienstverlening

We staan geen apps toe waarin gebruikers blootgesteld worden aan misleidende of schadelijke financiële producten en services.

Voor dit beleid definiëren we financiële producten en services als producten en services voor het beheren en investeren van geld en cryptocurrency's, waaronder gepersonaliseerd advies.

Als uw app financiële producten en services bevat of promoot, moet u voldoen aan de nationale en lokale regelgeving voor alle regio's en landen die uw app target (u moet bijvoorbeeld specifieke kennisgevingen opnemen zoals vereist door de lokale wetgeving).

Voor elke app die financiële functies bevat, moet het Declaratieformulier voor financiële functies in de Play Console worden ingevuld.

### Binaire opties

We staan geen apps toe die gebruikers de mogelijkheid bieden te handelen in binaire opties.

### Persoonlijke leningen

We definiëren een persoonlijke lening als het eenmalig verstrekken van een geldelijke lening door een persoon, organisatie of entiteit aan een individuele consument, die niet is bedoeld voor het financieren van de aankoop van vaste activa of onderwijs. Consumenten van persoonlijke leningen hebben informatie nodig over de kwaliteit, kenmerken, tarieven, aflossingsschema's, risico's en voordelen van leningen om weloverwogen beslissingen te kunnen nemen over het afsluiten van een lening.

- Voorbeelden zijn: persoonlijke leningen, salarisvoorschotten, peer-to-peer-leningen, en leningen op onderpand.
- Voorbeelden van leningen die hier niet onder vallen: hypotheken, autoleningen, doorlopend krediet (zoals creditcards, persoonlijke kredietlijnen).

Apps die persoonlijke leningen verstrekken, inclusief maar niet beperkt tot apps die rechtstreeks leningen aanbieden, apps waarmee leads kunnen worden gegenereerd en apps die consumenten in contact brengen met externe verstrekkers van leningen, moeten de app-categorie in de Play Console hebben ingesteld op Financieel, en de volgende informatie publiceren in de metadata van de app:

- De minimum- en maximumperiode voor terugbetaling.
- De maximale jaarlijkse rentevoet (APR), die over het algemeen de rentevoet plus vergoedingen en andere kosten voor een jaar omvat, of een vergelijkbare andere rentevoet die volgens de lokale wetgeving is berekend.
- Een representatief voorbeeld van de totale kosten van de lening, inclusief de hoofdsom en alle toepasselijke kosten.
- Een privacybeleid waarin het openen, verzamelen, gebruiken en delen van persoonsgegevens en gevoelige gebruikersgegevens volledig bekend wordt gemaakt, in overeenstemming met de

beperkingen die worden beschreven in dit beleid.

We staan geen apps toe die persoonlijke leningen promoten die binnen zestig (60) dagen of eerder na de uitgiftedatum van de lening volledig moeten worden terugbbetaald (we verwijzen hiernaar met de term 'kortlopende persoonlijke leningen').

We moeten een verband kunnen leggen tussen uw ontwikkelaarsaccount en de verstrekte licenties of documentatie waaruit blijkt dat u persoonlijke leningen mag aanbieden. We kunnen aanvullende informatie of documenten opvragen om te bevestigen dat uw account voldoet aan alle lokale wet- en regelgeving.

Apps voor persoonlijke leningen of apps die persoonlijke leningen mogelijk maken als hoofddoel hebben (dat wil zeggen, leadgenerators of -facilitators), mogen geen toegang hebben tot gevoelige gegevens, zoals foto's en contacten. De volgende rechten zijn niet toegestaan:

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

Apps die gebruikmaken van gevoelige informatie of API's vallen onder aanvullende beperkingen en vereisten. Bekijk het Beleid voor rechten voor meer informatie.

**Persoonlijke leningen met een hoge jaarlijkse rentevoet**

In de Verenigde Staten staan we geen apps toe voor persoonlijke leningen waarvoor de jaarlijkse rentevoet 36% of hoger is. Apps voor persoonlijke leningen in de Verenigde Staten moeten de maximum jaarlijkse rentevoet weergeven, berekend in overeenstemming met de Truth in Lending Act (TILA) .

Dit beleid is van toepassing op apps die rechtstreeks leningen aanbieden, apps waarmee leads kunnen worden gegenereerd en apps die consumenten in contact brengen met externe verstrekkers van leningen.

**Landspecifieke vereisten**

Apps voor persoonlijke leningen die de vermelde landen targeten, moeten voldoen aan aanvullende vereisten en aanvullende documentatie verstrekken als onderdeel van het Declaratieformulier voor financiële functies binnen de Play Console. Op verzoek van Google Play moet u aanvullende informatie of documenten verstrekken over de naleving van de toepasselijke regelgeving en licentievereisten.

1. **India**
   - Als u een licentie heeft van de Reserve Bank of India (RBI) om persoonlijke leningen te verstrekken, moet u een kopie van uw licentie indienen zodat wij deze kunnen beoordelen.
   - Als u niet rechtstreeks betrokken bent bij activiteiten in verband met het verstrekken van geldleningen en slechts een platform biedt dat de verstrekking van geldleningen door geregistreerde niet-bancaire financieringsbedrijven (NBFC, Non-Banking Finance Company) of banken aan gebruikers mogelijk maakt, moet u dit op nauwkeurige wijze vermelden in de verklaring.
     - Daarnaast moeten de namen van alle geregistreerde niet-bancaire financieringsbedrijven en banken door middel van een prominente kennisgeving in de beschrijving van uw app worden bekendgemaakt.
2. **Indonesië**

- Als uw app zich bezighoudt met activiteiten in het kader van kredietverleningsservices op basis van informatietechnologie (Information Technology-Based Money Lending Services) overeenkomstig OJK Regulation No. 77/POJK.01/2016 (die van tijd tot tijd kan worden aangepast), moet u een kopie van uw geldige licentie overleggen ter beoordeling.

3. **Filipijnen**
   - Alle financierings- en kredietverleningsbedrijven die leningen aanbieden via online kredietverleningsplatforms, moeten een SEC-registratienummer en het toestemmingscertificaatnummer (Certificate of Authority) verkrijgen van de Filipijnse Securities and Exchanges Commission (PSEC).
     - Daarnaast moet u uw bedrijfsnaam, handelsnaam, PSEC-registratienummer en het Toestemmingsformulier voor de exploitatie van een financierings-/kredietverleningsbedrijf (CA-nummer) bekendmaken in de beschrijving van uw app.
   - Apps waarbij sprake is van op kredietverlening gebaseerde crowdfundingactiviteiten, zoals kredietverlening tussen personen (P2P), of zoals gedefinieerd in de regels en verordeningen voor crowdfunding (de CF-regels), moeten transacties verwerken via bij de PSEC geregistreerde CF-tussenpersonen.

4. **Nigeria**
   - Digitale geldverstrekkers moeten zich houden aan en voldoen aan de LIMITED INTERIM REGULATORY/REGISTRATION FRAMEWORK AND GUIDELINES FOR DIGITAL LENDING, 2022 (die van tijd tot tijd kunnen worden aangepast) van de Nigeriaanse Federal Competition and Consumer Protection Commission (FCCPC) en een verifieerbare goedkeuringsbrief krijgen van de FCCPC.
   - Verzamelsites voor leningen moeten documentatie en/of certificering verstrekken voor digitale leenservices en contactgegevens voor elke digitale geldverstrekker waarmee ze samenwerken.

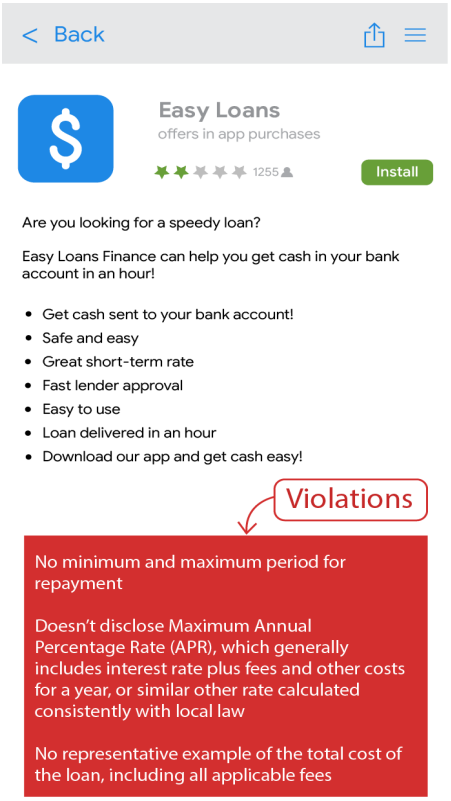
5. **Kenia**
   - Digitale kredietverstrekkers moeten het registratieproces voor digitale kredietverstrekkers doorlopen en een licentie krijgen van de Centrale Bank van Kenia (CBK). U moet een kopie van uw licentie van de CBK verstrekken als onderdeel van uw verklaring.
   - Als u niet rechtstreeks betrokken bent bij activiteiten in verband met het verstrekken van geldleningen en slechts een platform biedt dat de verstrekking van geldleningen door geregistreerde digitale kredietverstrekkers aan gebruikers mogelijk maakt, moet u dit op nauwkeurige wijze vermelden in de verklaring en een kopie van de licentie van uw respectieve partner(s) verstrekken.
   - Op dit moment accepteren we alleen verklaringen en licenties van entiteiten die zijn gepubliceerd in de Directory of Digital Credit Providers op de officiële website van de CBK.

6. **Pakistan**
   - Elke NBFC-geldverstrekker (Non-Banking Finance Company of niet-bancair financieringsbedrijf) mag maar één DLA (Digital Lending App) publiceren. Ontwikkelaars die proberen meer dan één DLA per NBFC te publiceren, lopen het risico dat hun ontwikkelaarsaccount en eventuele andere gekoppelde accounts worden beëindigd.
   - U moet een bewijs van goedkeuring van de SECP indienen om digitale leenservices aan te bieden of te faciliteren in Pakistan.

7. **Thailand**
   - Apps voor persoonlijke leningen die Thailand targeten, met rentetarieven van 15% of hoger, moeten een geldige licentie aanvragen bij de Bank of Thailand (BoT) of het Ministerie van Financiën (Ministry of Finance, MoF). Ontwikkelaars moeten documentatie verstrekken die aantoont dat ze persoonlijke leningen in Thailand kunnen leveren of mogelijk maken. Deze documentatie moet het volgende omvatten:
     - Een kopie van de door de Bank of Thailand uitgegeven licentie om te opereren als aanbieder van persoonlijke leningen of als organisatie voor nano-financiën.

- Een kopie van de door het Ministerie van Financiën uitgegeven Pico-finance-bedrijfslicentie om te opereren als Pico- of Pico-plus-kredietverstrekker.

We hebben normen opgesteld die content definiëren en verbieden die schadelijk of ongepast is voor onze gebruikers om ervoor te zorgen dat Google Play een veilig en respectvol platform blijft.




## Kansspelen, games en wedstrijden waarbij wordt gespeeld om echt geld

Apps waarmee kan worden gespeeld om echt geld, advertenties die verband houden met kansspelen waarbij wordt gespeeld om echt geld, loyaliteitsprogramma's met gamificatie en daily fantasy sport-apps zijn toegestaan als deze aan bepaalde vereisten voldoen.

### Kansspel-apps

Onder toepassing van beperkingen en onder voorbehoud van de naleving van alle beleidsregels van Google Play staan we in bepaalde landen apps toe die online kansspelen mogelijk maken, op voorwaarde dat de ontwikkelaar de aanvraagprocedure afrondt voor kansspel-apps die worden gedistribueerd op Google Play, een goedgekeurde overheidsaanbieder is en/of is geregistreerd als gelicentieerde aanbieder bij de toepasselijke kansspelautoriteit in het betreffende land en beschikt over een geldige licentie uit het betreffende land voor het type product voor online kansspelen dat de aanbieder wil leveren.

We staan alleen geldige gelicentieerde of geautoriseerde kansspel-apps toe die de volgende typen producten voor online kansspelen bevatten:

- Online casinogames
- Sportweddenschappen
- Paardenraces (indien deze afzonderlijk van sportweddenschappen worden gereguleerd en gelicentieerd)
- Loterijen
- Daily fantasy sports

In aanmerking komende apps moeten aan de volgende vereisten voldoen:

- de ontwikkelaar moet de aanvraagprocedure doorlopen om de app te distribueren op Google Play,
- de app moet voldoen aan alle toepasselijke wetten en branchenormen voor elk land waarin de app wordt gedistribueerd,
- de ontwikkelaar moet een geldige kansspellicentie hebben voor elk land of elke staat/regio waarin de app wordt gedistribueerd,
- de ontwikkelaar mag geen type kansspelproduct aanbieden dat het bereik van de kansspellicentie overschrijdt,
- de app moet voorkomen dat minderjarige gebruikers de app gebruiken,
- de app moet gebruik voorkomen vanuit landen, staten/regio's of geografische gebieden die niet vallen onder de door de ontwikkelaar geleverde kansspellicentie,
- de app mag NIET worden aangeboden als een betaalde app op Google Play. Ook mag de app niet gebruikmaken van in-app facturering via Google Play,
- de app moet kosteloos kunnen worden gedownload en geïnstalleerd vanuit de Google Play Store,
- de app moet zijn geclassificeerd als alleen voor volwassenen (of het IARC-equivalent daarvan),
- de app en bijbehorende app-vermelding moeten duidelijke informatie weergeven over een verantwoordelijke benadering van kansspelen.

## Andere apps voor games, wedstrijden en toernooien om echt geld

Voor alle andere apps die niet voldoen aan de deelnamevereisten voor kansspel-apps die hierboven worden vermeld en die geen deel uitmaken van de 'Pilots voor andere games om echt geld' zoals hieronder worden vermeld, staan we geen content of services toe waarmee gebruikers kunnen inzetten, wedden of deelnemen met echt geld (waaronder in-app-items die zijn gekocht met geld) om een prijs in geldwaarde te ontvangen. Dit omvat, maar is niet beperkt tot, online casino's, sportweddenschappen, loterijen, en games die geld accepteren en prijzen in contant geld of andere echte waarde bieden (met uitzondering van programma's die zijn toegestaan volgens de hieronder beschreven vereisten voor loyaliteitsprogramma's met gamificatie).

### Voorbeelden van schendingen

- Games die geld accepteren in ruil voor een kans om een fysieke of geldprijs te winnen.
- Apps met navigatie-elementen of functies (bijvoorbeeld menu-items, tabbladen, knoppen, WebViews, enzovoort) die een call-to-action bieden om met echt geld in te zetten op, te wedden op of deel te nemen aan games, wedstrijden of toernooien, zoals apps die gebruikers uitnodigen om te wedden (ZET NU IN), zich te registreren (REGISTREER NU) of deel te nemen (DOE NU MEE) aan een toernooi om kans te maken op een geldprijs.
- Apps die de inzet van kansspelen, in-app-valuta's, winst of stortingen accepteren of beheren om kans te maken op een fysieke of geldprijs.

### Pilots voor andere games om echt geld

We kunnen af en toe in bepaalde regio's tijdelijke pilots uitvoeren voor bepaalde soorten kansspelen waarbij wordt gespeeld om echt geld. Ga naar deze pagina in het Helpcentrum voor meer informatie. De pilot voor online grijpautomaatgames in Japan is op 11 juli 2023 beëindigd. Vanaf 12 juli 2023 kunnen apps voor online grijpautomaatgames wereldwijd op Google Play worden vermeld. Hierop zijn toepasselijke wetgeving en bepaalde vereisten van toepassing.

## Loyaliteitsprogramma's met gamificatie

Als dit wettelijk is toegestaan en niet onder aanvullende vereisten voor kansspel- of gamelicenties valt, staan we loyaliteitsprogramma's toe die gebruikers belonen met echte prijzen of een equivalent van de geldwaarde, in overeenstemming met de volgende deelnamevereisten voor de Play Store:

**Voor alle apps (games en niet-games):**

- (Speciale) voordelen of beloningen van loyaliteitsprogramma's moeten duidelijk een aanvulling vormen op en ondergeschikt zijn aan een in aanmerking komende geldtransactie binnen de app (waarbij de in aanmerking komende geldtransactie een echt afzonderlijke transactie moet zijn om goederen of services te leveren die losstaan van het loyaliteitsprogramma). Ze mogen niet onderhevig zijn aan een aankoop of zijn gekoppeld aan een uitwisseling die anderszins in strijd is met de beperkingen van het beleid Kansspelen, games en wedstrijden waarbij wordt gespeeld om echt geld.
  - Geen enkel deel van de in aanmerking komende geldtransactie mag bijvoorbeeld kosten of een inzet vertegenwoordigen om deel te nemen aan het loyaliteitsprogramma, en de in aanmerking komende geldtransactie mag niet leiden tot de aankoop van goederen of services boven de normale prijs.

**Voor game -apps:**

- Spaarpunten of beloningen met (speciale) voordelen of beloningen die horen bij een in aanmerking komende geldtransactie mogen alleen worden toegekend en ingewisseld op basis van een vaste verhouding, waarbij de verhouding duidelijk wordt gedocumenteerd in de app en ook binnen de openbaar beschikbare officiële regels voor het programma. De opbrengst van beloningen of inwisselbare waarde mag **niet** worden ingezet, toegekend of geëxponentieerd door gameprestaties of op kans gebaseerde resultaten.

**Voor niet-game-apps:**

- Spaarpunten of beloningen mogen worden gekoppeld aan een wedstrijd of op kans gebaseerde resultaten als ze aan de onderstaande vereisten voldoen. Het volgende is van toepassing op loyaliteitsprogramma's met (speciale) voordelen of beloningen die horen bij een in aanmerking komende geldtransactie:
  - De officiële regels voor het programma moeten worden gepubliceerd in de app.
  - Voor programma's met variabele, op kans gebaseerde of willekeurige beloningssystemen: in de officiële voorwaarden voor het programma moet het volgende openbaar worden gemaakt 1) hoe groot de kans is om beloningen te winnen voor eventuele beloningsprogramma's die vaste kansen gebruiken en 2) de selectiemethode (bijv. variabelen die worden gebruikt om de beloning te winnen) voor alle andere programma's.
  - Er moeten een vast aantal winnaars, een vaste deadline en een uitreikingsdatum voor de prijs worden aangegeven (per promotie) in de officiële voorwaarden van een programma met prijstrekkingen, sweepstakes of soortgelijke promoties.
  - Geef duidelijk in de app en in de officiële voorwaarden van het programma een vaste verhouding op voor het verzamelen en inwisselen van spaarpunten of loyaliteitsbeloningen.

| **Type app met loyaliteitsprogramma** | **Loyaliteitsprogramma met gamificatie en variabele beloningen** | **Loyaliteitsbeloningen op basis van een vaste verhouding/vast schema** | **Algemene Voorwaarden van het loyaliteitsprogramma vereist** | **Algem Voorw de kan selecti elk op gebas loyalit openb** |
|---|---|---|---|---|
| Game | Niet toegestaan | Toegestaan | Vereist | N.v.t. (g mogen gebase elemer loyalite hebber |
| Niet-game | Toegestaan | Toegestaan | Vereist | Vereist |

## Advertenties voor kansspelen of games, wedstrijden of toernooien waarbij om echt geld wordt gespeeld in op Play gedistribueerde apps

We staan apps toe met advertenties voor kansspelen of games, wedstrijden of toernooien waarbij om echt geld wordt gespeeld als ze voldoen aan de volgende vereisten:

- de app en advertentie (waaronder adverteerders) moeten voldoen aan alle toepasselijke wetten en branchenormen voor elke locatie waar de advertentie wordt getoond,
- de advertentie moet voldoen aan alle toepasselijke lokale advertentielicentievereisten voor alle kansspelgerelateerde producten en services die worden gepromoot,
- de app mag geen kansspeladvertenties laten zien aan gebruikers waarvan bekend is dat ze jonger dan 18 jaar zijn,
- de app mag niet zijn aangemeld voor het programma Gemaakt voor gezinnen,
- de app mag geen gebruikers targeten die jonger dan 18 jaar zijn,
- als er reclame wordt gemaakt voor een kansspel-app (zoals hierboven gedefinieerd), moet de advertentie op de landingspagina, in de vermelding van de geadverteerde app of in de app zelf duidelijke informatie laten zien over een verantwoordelijke benadering van kansspelen,
- de app mag geen gesimuleerde content met betrekking tot kansspelen aanbieden (zoals sociale casino-apps, apps met virtuele gokautomaten),
- de app mag geen begeleidende of ondersteuningsfunctionaliteit bieden voor kansspelen of games, wedstrijden of toernooien waarbij om echt geld wordt gespeeld (zoals functionaliteit voor hulp bij gokken, uitbetalingen, het bijhouden van sportscores/kansberekening/prestaties of het beheren van deelnamegeld),
- app-content mag geen kansspelservices of games, loterijen of toernooien waarbij om echt geld wordt gespeeld, promoten of gebruikers naar deze services leiden.

Alleen apps die aan alle vereisten in het vermelde gedeelte (hierboven) voldoen, mogen advertenties bevatten voor kansspelen of games, loterijen of toernooien waarbij om echt geld wordt gespeeld. Geaccepteerde kansspel-apps (zoals hierboven gedefinieerd) of geaccepteerde daily fantasy sport-apps (zoals hieronder gedefinieerd) die voldoen aan de vereisten 1-6 hierboven, mogen advertenties bevatten voor kansspelen of games, loterijen of toernooien waarbij om echt geld wordt gespeeld.

**Voorbeelden van schendingen**

- Een app die is ontworpen voor minderjarige gebruikers en waarin een advertentie wordt getoond waarin kansspelservices worden gepromoot.
- Een gesimuleerde casinogame die casino's waar wordt gespeeld om echt geld promoot of die gebruikers naar dergelijke casino's leidt.
- Een speciale app voor het bijhouden van kansberekening in sport met geïntegreerde kansspeladvertenties die een link bevatten naar een site voor sportweddenschappen.
- Apps met kansspeladvertenties die ons beleid Misleidende advertenties schenden, zoals advertenties die aan gebruikers worden getoond als knoppen, iconen of andere interactieve in-app-elementen.

## Daily fantasy sport-apps (DFS)

We staan daily fantasy sport-apps (DFS), zoals gedefinieerd in de toepasselijke lokale wetgeving, alleen toe als ze voldoen aan de volgende vereisten:

- de app wordt 1) alleen gedistribueerd in de Verenigde Staten of 2) komt op grond van de hierboven genoemde vereisten en aanvraagprocedure voor kansspel-apps in aanmerking voor andere landen dan de Verenigde Staten,
- de ontwikkelaar moet de DFS-aanvraagprocedure doorlopen en worden geaccepteerd om de app op Google Play te kunnen distribueren,

- de app moet voldoen aan alle toepasselijke wetgeving en branchenormen voor de landen waar de app wordt gedistribueerd,
- de app moet voorkomen dat minderjarige gebruikers wedden of geldtransacties uitvoeren in de app,
- de app mag NIET worden aangeboden als een betaalde app op Google Play. Ook mag de app niet gebruikmaken van in-app-facturering via Google Play,
- de app moet gratis kunnen worden gedownload en geïnstalleerd vanuit de Google Play Store,
- de app moet zijn geclassificeerd als alleen voor volwassenen (of het IARC-equivalent daarvan),
- de app en bijbehorende app-vermelding moeten duidelijke informatie bevatten over een verantwoordelijke benadering van kansspelen,
- de app moet voldoen aan alle toepasselijke wetten en branchenormen voor elke staat in en elk grondgebied van de Verenigde Staten waar de app wordt gedistribueerd,
- de ontwikkelaar moet beschikken over een geldige licentie voor elke staat in en elk grondgebied van de Verenigde Staten waar een licentie vereist is voor daily fantasy sport-apps,
- de app moet voorkomen dat deze kan worden gebruikt in staten in of grondgebieden van de Verenigde Staten waar de ontwikkelaar niet beschikt over een licentie die is vereist voor daily fantasy sport-apps,
- de app moet voorkomen dat deze kan worden gebruikt in staten in of grondgebieden van de Verenigde Staten waar daily fantasy sport-apps niet legaal zijn.

---

## Illegale activiteiten

We staan geen apps toe die illegale activiteiten faciliteren of promoten.

We hebben normen opgesteld die content definiëren en verbieden die schadelijk of ongepast is voor onze gebruikers om ervoor te zorgen dat Google Play een veilig en respectvol platform blijft.

- Ondersteuning van de verkoop of aankoop van illegale drugs.
- Afbeelding of aanmoediging van het gebruik of de verkoop van drugs, alcohol of tabak door minderjarigen.
- Instructies voor het kweken of vervaardigen van illegale drugs.

---

## Door gebruikers gegenereerde content

Door gebruikers gegenereerde content (UGC) is content die gebruikers bijdragen aan een app en die zichtbaar of toegankelijk is voor ten minste een groep gebruikers van de app.

Apps die UGC bevatten of tonen, waaronder apps zoals gespecialiseerde browsers of clients om gebruikers naar een UGC-platform te leiden, moeten robuuste, doeltreffende en voortdurende moderatie van UGC implementeren die:

- vereist dat gebruikers de gebruiksvoorwaarden en/of het gebruikersbeleid van de app accepteren voordat gebruikers UGC kunnen maken of uploaden,
- aanstootgevende content en gedrag definieert (op een manier die voldoet aan het Programmabeleid voor ontwikkelaars van Google Play) en deze verbiedt in de gebruiksvoorwaarden of het gebruikersbeleid van de app,
- UGC-content beheren, voor zover redelijk en consistent is met de soorten UGC die de app host. Dit omvat onder meer het bieden van een in-app systeem om aanstootgevende UGC en gebruikers te melden en te blokkeren en zo nodig actie ondernemen tegen die UGC of gebruikers. Verschillende UGC-functies moeten mogelijk op verschillende manieren worden beheerd. Bijvoorbeeld:
  - apps met UGC waarin een specifieke set gebruikers wordt geïdentificeerd met behulp van bijvoorbeeld gebruikersverificatie of offline registratie (zoals apps die uitsluitend worden gebruikt binnen een specifieke school of een specifiek bedrijf, enz.) moeten in-app functies bevatten om content en gebruikers te melden,

- UGC-functies waarmee 1-op-1 gebruikersinteractie mogelijk is met specifieke gebruikers (zoals privéchats, taggen, vermeldingen, enz.) moeten in-app functies bieden om gebruikers te blokkeren,
- apps die toegang bieden tot openbaar toegankelijke UGC, zoals sociaal netwerk-apps en blogger-apps, moeten in-app functies bieden om gebruikers en content te melden en om gebruikers te blokkeren,
- in het geval van AR-apps (augmented reality) zorgen dat de UGC-moderatie (inclusief het meldingssysteem in apps) rekening houdt met zowel aanstootgevende AR-UGC (bijvoorbeeld een seksueel expliciete AR-afbeelding) als gevoelige AR-ankerlocatie (bijvoorbeeld AR-content die is verankerd in een gebied dat niet toegankelijk is, zoals een militaire basis of een privéterrein waar AR-verankering problemen kan veroorzaken voor de eigenaar van de locatie),

- waarborgt dat in de app geen inkomsten kunnen worden gegenereerd door het stimuleren van aanstootgevend gedrag van gebruikers.

**Incidentele seksuele content**

Seksuele content wordt beschouwd als 'incidenteel' als het wordt getoond in een UGC-app die (1) toegang biedt tot voornamelijk niet-seksuele content, en (2) seksuele content niet op actieve wijze promoot of aanbeveelt. Seksuele content die in de toepasselijke wetgeving wordt gedefinieerd als illegaal en content die kinderen in gevaar brengt, worden niet beschouwd als 'incidenteel' en zijn niet toegestaan.

UGC-apps mogen incidentele seksuele content bevatten als aan alle volgende vereisten is voldaan:

- Dergelijke content is standaard verborgen achter filters die uitsluitend na minimaal 2 gebruikersacties kunnen worden uitgezet (zoals achter een verhullende interstitial of standaard niet zichtbaar tenzij SafeSearch uitstaat).
- Het is kinderen, zoals gedefinieerd in het Gezinsbeleid, uitdrukkelijk niet toegestaan toegang te krijgen tot uw app via systemen voor leeftijdscontrole, zoals een neutraal leeftijdsscherm of een ander geschikt systeem zoals gedefinieerd in de toepasselijke wetgeving.
- Uw app verstrekt nauwkeurige antwoorden in de vragenlijst voor contentclassificatie met betrekking tot UGC, zoals vereist in het Beleid voor contentclassificatie.

Apps met het hoofddoel bezwaarlijke UGC te tonen, worden verwijderd uit Google Play. Ook apps die uiteindelijk hoofdzakelijk worden gebruikt voor het hosten van bezwaarlijke UGC of die onder gebruikers de reputatie ontwikkelen dat het een geschikte plek is voor dat soort content, worden verwijderd uit Google Play.

We hebben normen opgesteld die content definiëren en verbieden die schadelijk of ongepast is voor onze gebruikers om ervoor te zorgen dat Google Play een veilig en respectvol platform blijft.

- Seksueel expliciete content die is gemaakt door gebruikers promoten, waaronder de implementatie of het toestaan van betaalde functies die voornamelijk tot doel hebben het delen van aanstootgevende content te stimuleren.
- Apps met door gebruikers gegenereerde content die onvoldoende beschermingsmaatregelen bevatten tegen bedreigingen, intimidatie of pesten, in het bijzonder tegen minderjarigen.
- Posts, reacties of foto's plaatsen met een app die primair bedoeld zijn om een andere persoon te intimideren of aan te merken voor misbruik, kwaadwillende aanvallen of bespotting.
- Apps die klachten van gebruikers over bezwaarlijke content voortdurend negeren.

---

## Content over en services voor gezondheid

We staan geen apps toe die gebruikers blootstellen aan schadelijke content over en services voor gezondheid.

Als uw app content over en services voor gezondheid bevat of promoot, moet u ervoor zorgen dat uw app voldoet aan alle toepasselijke wet- en regelgeving.

### Geneesmiddelen op recept

We staan geen apps toe die de verkoop of aanschaf van geneesmiddelen op recept mogelijk maken zonder recept.

### Niet-goedgekeurde stoffen

Google Play staat geen apps toe die niet-goedgekeurde stoffen promoten of verkopen, ongeacht claims over de legaliteit.

We hebben normen opgesteld die content definiëren en verbieden die schadelijk of ongepast is voor onze gebruikers om ervoor te zorgen dat Google Play een veilig en respectvol platform blijft.

- Alle items op deze niet-volledige lijst met verboden farmaceutische producten en supplementen .
- Producten die efedra bevatten.
- Producten die hCG (humaan choriongonadotrofine) bevatten in verband met gewichtsverlies of gewichtsbeheersing of indien gepromoot in combinatie met anabole steroïden.
- Kruiden- en dieetsupplementen met actieve farmaceutische of gevaarlijke ingrediënten.
- Onjuiste of misleidende gezondheidsclaims, waaronder claims die impliceren dat een product even effectief is als geneesmiddelen op recept of gereguleerde stoffen.
- Producten die niet door de overheid zijn goedgekeurd en die worden gepromoot alsof ze veilig of effectief zijn ter voorkoming, behandeling of genezing van een bepaalde ziekte of aandoening.
- Producten waartegen overheden of regulerende instanties waarschuwen of acties ondernemen.
- Producten met namen die een verwarrende gelijkenis vertonen met een niet-goedgekeurd farmaceutisch product of supplement of gereguleerde stof.

Ga naar www.legitscript.com voor meer informatie over de niet-goedgekeurde of misleidende farmaceutische producten en supplementen die we controleren.

### Misleidende gezondheidsinformatie

We staan geen apps toe met misleidende claims over gezondheid die strijdig zijn met de bestaande medische consensus of die gebruikers schade kunnen berokkenen.

We hebben normen opgesteld die content definiëren en verbieden die schadelijk of ongepast is voor onze gebruikers om ervoor te zorgen dat Google Play een veilig en respectvol platform blijft.

- Misleidende claims over vaccins, zoals dat vaccins iemands dna kunnen veranderen.
- Promoten van schadelijke, niet-goedgekeurde behandelingen.
- Promoten van andere schadelijke gezondheidspraktijken, zoals conversietherapie.

### COVID-19-beperkingen

Apps moeten zich houden aan de vereisten voor COVID-19-apps (coronavirus 2019) .

### Medische functies

We staan geen apps toe met medische of gezondheidsgerelateerde functies die misleidend of mogelijk schadelijk zijn. We staan bijvoorbeeld geen apps toe die claimen te beschikken over oximetriefuncties die uitsluitend app-gebaseerd zijn. Oximeter-apps moeten worden ondersteund door externe hardware, wearables of specifieke smartphonesensoren die zijn ontworpen om de oximetriefunctie te ondersteunen. Deze ondersteunde apps moeten ook disclaimers bevatten in de metadata waarin staat dat zij niet bestemd zijn voor medisch gebruik, alleen zijn ontworpen voor algemene fitness- en welzijnsdoeleinden en geen medisch hulpmiddel zijn. Ook moeten ze het geschikte hardwaremodel/apparaatmodel duidelijk bekendmaken.

### Betalingen - Klinische services

Het factureringssysteem van Google Play mag niet worden gebruikt voor transacties met betrekking tot gereguleerde klinische services. Raadpleeg voor meer informatie het Betalingsbeleid van Google Play .

#### Health Connect-gegevens

Gegevens waartoe toegang wordt verkregen via de rechten voor Health Connect worden beschouwd als persoonsgegevens en gevoelige gebruikersgegevens waarop het beleid voor Gebruikersgegevens en aanvullende vereisten van toepassing zijn.

---

## Content op basis van blockchains

De ontwikkeling van blockchain-technologie gaat razendsnel. Daarom willen we ontwikkelaars een platform bieden waar ze verder kunnen groeien door innovatie en ontwikkeling van uitgebreidere, immersievere belevingen voor gebruikers.

Voor dit beleid beschouwen we content op basis van blockchains als digitale middelen op basis van tokens die via een blockchain worden aangeboden. Als uw app content op basis van blockchains bevat, moet u aan deze vereisten voldoen.

#### Cryptocurrencybeurzen en software-wallets

De aankoop, het bezit of de uitwisseling van cryptocurrency's moet worden uitgevoerd via gecertificeerde services in gereguleerde jurisdicties.

U moet ook de toepasselijke regelgeving naleven voor elke regio of elk land dat door uw app wordt getarget en u moet voorkomen dat uw app wordt gepubliceerd in gebieden waar uw producten of services verboden zijn. Google Play kan u vragen aanvullende informatie of documentatie te verstrekken met betrekking tot uw naleving van toepasselijke regelgevende of licentievereisten.

#### Cryptomining

We staan geen apps toe die cryptocurrency minen op een apparaat. We staan wel apps toe die het minen van cryptocurrency op afstand beheren.

#### Transparantievereisten voor de distributie van digitale middelen op basis van tokens

Als uw app digitale middelen op basis van tokens verkoopt of gebruikers in staat stelt deze middelen te verdienen, moet u dit aangeven via het Declaratieformulier voor financiële functies op de pagina App-content in de Play Console.

Als u een in-app product maakt, moet u in de productdetails aangeven dat dit een digitaal middel op basis van tokens vertegenwoordigt. Zie Een in-app product maken voor meer informatie.

U mag mogelijke verdiensten die voortvloeien uit speel- of ruilactiviteiten niet promoten of mooier laten lijken.

#### Aanvullende vereisten voor NFT-gamificatie

Zoals vereist door het Google Play-beleid voor kansspelen, games en wedstrijden waarbij wordt gespeeld om echt geld, moeten apps voor kansspelen met integratie van digitale middelen op basis van tokens, zoals NFT's, het aanvraagproces afronden.

Voor alle andere apps die niet voldoen aan de deelnamevereisten voor apps voor kansspelen en die niet zijn toegevoegd aan pilots voor andere games om echt geld, mag niets van geldwaarde worden geaccepteerd in ruil voor een kans om een NFT van onbekende waarde te verkrijgen. Door gebruikers gekochte NFT's moeten in de game worden gebruikt om de beleving van de gebruiker te verrijken of gebruikers te helpen verder te komen in de game. NFT's mogen niet worden gebruikt als aandeel of inzet in ruil voor de mogelijkheid om prijzen met echte geldwaarde (waaronder andere NFT's) te winnen.

We hebben normen opgesteld die content definiëren en verbieden die schadelijk of ongepast is voor onze gebruikers om ervoor te zorgen dat Google Play een veilig en respectvol platform blijft.

- Apps die NFT-bundels verkopen zonder de specifieke content en waarde van de NFT's bekend te maken.
- Sociale casinogames op basis van pay-to-play, zoals gokautomaten, die NFT's als beloning verstrekken.

---

### Door AI gemaakte content

Met de steeds bredere beschikbaarheid van generatieve AI-modellen voor ontwikkelaars, past u deze modellen mogelijk toe in uw apps om de betrokkenheid van gebruikers te vergroten en de gebruikerservaring te verbeteren. Google Play wil helpen ervoor te zorgen dat door AI gemaakte content veilig is voor alle gebruikers en dat de feedback van gebruikers wordt gebruikt om verantwoordelijke innovatie mogelijk te maken.

#### Door AI gemaakte content

Door AI gemaakte content is content die is gemaakt door generatieve AI-modellen op basis van prompts van de gebruiker. Voorbeelden van door AI gemaakte content zijn onder meer:

- generatieve AI-chatbots die werken op basis van geschreven gesprekken, waarbij de interactie met de chatbot een centrale functie is van de app,
- afbeeldingen die worden gegenereerd door AI op basis van tekst-, afbeeldings- of gesproken prompts

In overeenstemming met de beleidsdekking van Google Play en om de veiligheid van gebruikers te waarborgen, moeten apps die content genereren met behulp van AI voldoen aan het bestaande beleid voor ontwikkelaars van Google Play, waaronder door het genereren van beperkte content, zoals content die de uitbuiting of misbruik van kinderen mogelijk maakt, en content die misleidend gedrag mogelijk maakt te verbieden en te voorkomen.

Apps die content genereren met behulp van AI moeten in de app meld- of markeerfuncties bevatten waarmee gebruikers aanstootgevende content kunnen melden of markeren voor de ontwikkelaars, zonder dat zij de app hoeven te verlaten. Ontwikkelaars moeten mede op basis van de meldingen van gebruikers content in hun apps filteren en beheren.

---

## Intellectueel eigendom

We staan geen apps of ontwikkelaarsaccounts toe die inbreuk maken op de intellectuele-eigendomsrechten van anderen (waaronder handelsmerken, auteursrechten, patenten, handelsgeheimen en andere eigendomsrechten). We staan ook geen apps toe die inbreuk op intellectuele-eigendomsrechten stimuleren of veroorzaken.

We reageren op duidelijke meldingen van vermeende inbreuk op auteursrecht. Raadpleeg onze auteursrechtprocedures voor meer informatie of voor het indienen van een DMCA-verzoek.

Als u een klacht wilt indienen over de verkoop en promotie van namaakartikelen in een app, kunt u een melding van namaakartikelen indienen.

Als u de eigenaar bent van een handelsmerk en van mening bent dat er op Google Play een app beschikbaar is die inbreuk maakt op uw handelsmerkrechten, raden we u aan rechtstreeks contact op te nemen met de ontwikkelaar om uw zorgen kenbaar te maken. Als u niet tot een oplossing kunt komen met de ontwikkelaar, kunt u via dit formulier een handelsmerkklacht indienen.

Als u schriftelijke documentatie heeft die aantoont dat u over de rechten beschikt om de intellectuele eigendom van derden te gebruiken in uw app of winkelvermelding (zoals merknamen en logo's en grafische items), neemt u contact op met het Google Play-team voordat u uw klacht indient, om er

zeker van te zijn dat uw app niet wordt geweigerd op grond van een schending van intellectuele eigendom.

## Onbevoegd gebruik van auteursrechtelijk beschermd materiaal

We staan geen apps toe die inbreuk maken op een auteursrecht. Ook na het aanpassen van auteursrechtelijk beschermd materiaal kan er nog steeds sprake zijn van schending. Ontwikkelaars kan worden gevraagd bewijs te leveren van hun rechten voor het gebruik van auteursrechtelijk beschermd materiaal.

Wees voorzichtig bij het gebruik van auteursrechtelijk beschermde content om de functionaliteit van uw app aan te tonen. Over het algemeen is het veiliger om originele content te maken.

We hebben normen opgesteld die content definiëren en verbieden die schadelijk of ongepast is voor onze gebruikers om ervoor te zorgen dat Google Play een veilig en respectvol platform blijft.

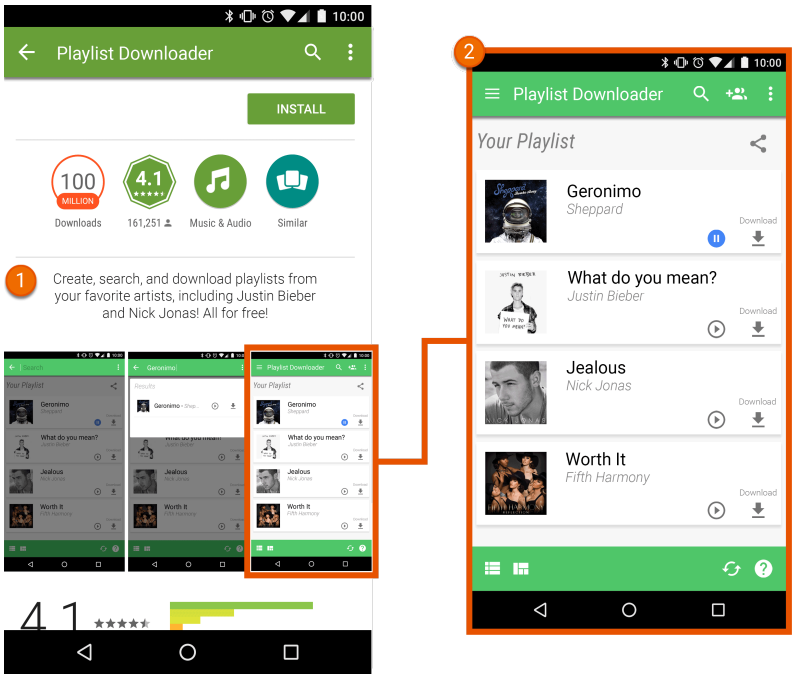
- omslagen/hoezen voor muziekalbums, videogames en boeken,
- marketingafbeeldingen uit films, televisieprogramma's of videogames,
- afbeeldingen uit stripboeken, tekenfilms, films, muziekvideo's of televisieprogramma's,
- logo's van amateur- of professionele sportteams,
- foto's die afkomstig zijn van het social media-account van een bekende persoon,
- professionele afbeeldingen van bekende personen,
- reproducties of 'fan art' die niet te onderscheiden zijn van het oorspronkelijke auteursrechtelijk beschermde werk,
- apps met soundboards die audiofragmenten afspelen uit auteursrechtelijk beschermd materiaal,
- volledige reproducties of vertalingen van boeken die zich niet in het publieke domein bevinden.

## Stimuleren van inbreuk op auteursrecht

We staan geen apps toe die auteursrechtschending veroorzaken of stimuleren. Voordat u uw app publiceert, moet u onderzoeken of er manieren zijn waarop uw app auteursrechtschending stimuleert. Vraag indien nodig om juridisch advies.

We hebben normen opgesteld die content definiëren en verbieden die schadelijk of ongepast is voor onze gebruikers om ervoor te zorgen dat Google Play een veilig en respectvol platform blijft.

- Streaming-apps waarmee gebruikers een lokale kopie van auteursrechtelijk beschermd materiaal kunnen downloaden zonder toestemming.
- Apps die het streamen en downloaden van auteursrechtelijk beschermd materiaal stimuleren, met inbegrip van muziek en video, in strijd met de toepasselijke auteursrechtwetgeving:




① De beschrijving in deze app-vermelding stimuleert gebruikers om auteursrechtelijk beschermd materiaal te downloaden zonder toestemming.
② Het screenshot in de app-vermelding stimuleert gebruikers om auteursrechtelijk beschermd materiaal te downloaden zonder toestemming.

### Inbreuk op handelsmerk

We staan geen apps toe die inbreuk maken op de handelsmerken van anderen. Een handelsmerk is een woord, symbool of een combinatie hiervan waarmee de bron van een goed of service wordt geïdentificeerd. Zodra een handelsmerk is verkregen, geeft dit de eigenaar het exclusieve recht op het gebruik van het handelsmerk met betrekking tot bepaalde goederen of services.

Inbreuk op een handelsmerk vindt plaats wanneer er sprake is van onjuist of onbevoegd gebruik van een identiek of soortgelijk handelsmerk op zo'n manier dat het waarschijnlijk is dat er verwarring ontstaat over de bron van dat product. Als uw app handelsmerken van andere partijen gebruikt en dit tot verwarring kan leiden, kan uw app worden opgeschort.

### Namaak

We staan geen apps toe die namaakartikelen verkopen of de verkoop ervan promoten. Namaakartikelen zijn voorzien van een handelsmerk of logo dat niet of nauwelijks te onderscheiden is van het handelsmerk van iemand anders. Deze artikelen bevatten geïmiteerde merkkenmerken van het product met het doel ze te promoten als officiële producten van de merkeigenaar.

---

## Privacy, misleiding en apparaatmisbruik

We streven ernaar de privacy van gebruikers te beschermen en een veilige omgeving te bieden aan onze gebruikers. Apps die misleidend of kwaadwillend zijn of die een netwerk, apparaat of persoonlijke gegevens misbruiken, zijn ten strengste verboden.

### Gebruikersgegevens

U moet transparant zijn over hoe u omgaat met gebruikersgegevens (zoals gegevens die worden verzameld van of over een gebruiker, waaronder apparaatgegevens). Dit houdt in dat u bekendmaakt of en hoe er toegang wordt gekregen tot gebruikersgegevens in uw app, en hoe deze worden

verzameld, gebruikt, verwerkt en gedeeld, en dat u het gebruik van de gegevens beperkt tot de bekendgemaakte en beleidsconforme doeleinden. We wijzen u erop dat op de verwerking van persoonsgegevens en gevoelige gebruikersgegevens aanvullende vereisten van toepassing zijn overeenkomstig het onderstaande gedeelte Persoonsgegevens en gevoelige gebruikersgegevens. Deze vereisten voor Google Play gelden in aanvulling op eventuele vereisten die worden voorgeschreven in de toepasselijke wetgeving op het gebied van privacy en gegevensbescherming.

Als u code van derden (zoals een SDK) opneemt in uw app, moet u ervoor zorgen dat de code van derden die in uw app wordt gebruikt en de praktijken van die derde met betrekking tot de gebruikersgegevens uit uw app voldoen aan het Programmabeleid voor ontwikkelaars van Google Play, dat onder meer gebruiks- en kennisgevingsvereisten bevat. U moet er bijvoorbeeld voor zorgen dat uw SDK-providers geen persoonsgegevens en gevoelige gebruikersgegevens uit uw app verkopen. Deze vereiste is van toepassing ongeacht of gebruikersgegevens worden overgedragen nadat ze naar een server zijn gestuurd of door de insluiting van code van derden in uw app.

**Persoonsgegevens en gevoelige gebruikersgegevens**

Persoonsgegevens en gevoelige gebruikersgegevens omvatten onder meer persoonlijk identificeerbare informatie, financiële en betalingsgegevens, verificatie-informatie, het telefoonboek, contacten, de apparaatlocatie , gegevens over sms-berichten en gesprekken, gezondheidsgegevens , Health Connect -gegevens, welke andere apps op het apparaat staan, de microfoon, de camera en andere gevoelige apparaat- of gebruiksgegevens. Als uw app met persoonsgegevens of gevoelige gebruikersgegevens werkt, moet u het volgende doen:

- De toegang tot persoonsgegevens en gevoelige gebruikersgegevens die worden verkregen via de app en de verzameling, het gebruik en het delen ervan, beperken tot de app- en servicefuncties en beleidsconforme doeleinden die de gebruiker redelijkerwijs kan verwachten:
  - Apps die het gebruik van persoonsgegevens en gevoelige gebruikersgegevens uitbreiden voor de weergave van advertenties, moeten voldoen aan het Advertentiebeleid van Google Play.
  - U kunt voor zover nodig ook gegevens overdragen aan serviceproviders of om juridische redenen, bijvoorbeeld om te voldoen aan een geldig overheidsverzoek, de toepasselijke wetgeving of als onderdeel van een fusie of overname met een juridisch toereikende kennisgeving aan gebruikers.
- Beveiligd werken met alle persoonsgegevens en gevoelige gebruikersgegevens, inclusief overdragen van de gegevens met behulp van moderne versleuteling (bijvoorbeeld via https).
- Waar mogelijk een verzoek om runtimerechten gebruiken voordat toegang wordt verkregen tot gegevens die worden afgeschermd door Android-rechten .
- Geen persoonsgegevens en gevoelige gebruikersgegevens verkopen.
  - Onder 'verkoop' wordt verstaan: De uitwisseling of overdracht van persoonsgegevens en gevoelige gebruikersgegevens aan een derde voor een geldelijke vergoeding.
    - Een door de gebruiker gestarte overdracht van persoonsgegevens en gevoelige gebruikersgegevens wordt niet beschouwd als verkoop (bijvoorbeeld als de gebruiker een functie in de app gebruikt om een bestand over te dragen aan een derde of als de gebruiker ervoor kiest een specifieke app te gebruiken voor speciale onderzoeksdoeleinden).

**Vereisten voor prominente kennisgeving en toestemming**

Wanneer de toegang van uw app tot persoonsgegevens en gevoelige gebruikersgegevens of het verzamelen, gebruiken of delen ervan niet binnen de redelijke verwachting van de gebruiker van het betreffende product of de betreffende functie valt (als er bijvoorbeeld gegevens worden verzameld op de achtergrond terwijl de gebruiker de app op dat moment niet gebruikt), moet u aan de volgende vereisten voldoen:

**Prominente kennisgeving: U moet in de app een kennisgeving verstrekken over uw toegang tot, en het verzamelen, gebruiken en delen van gegevens. De kennisgeving in de app:**

- moet in de app zelf worden getoond, niet alleen in de beschrijving van de app of op een website,

- moet worden getoond tijdens normaal gebruik van de app en mag niet vereisen dat de gebruiker naar een menu of de instellingen navigeert,
- moet beschrijven tot welke gegevens toegang wordt verkregen of welke gegevens worden verzameld,
- moet een uitleg bevatten van hoe de gegevens worden gebruikt en/of gedeeld,
- mag niet alleen in een privacybeleid of servicevoorwaarden worden geplaatst, en
- mag geen deel uitmaken van andere kennisgevingen die niet gerelateerd zijn aan de verzameling van persoonsgegevens en gevoelige gebruikersgegevens.

**Toestemming en runtime-rechten: Direct voorafgaand aan verzoeken voor gebruikerstoestemming in de app en verzoeken om runtime-rechten moet een kennisgeving worden getoond die voldoet aan de vereisten in dit beleid. Het verzoek om toestemming in de app:**

- moet in het toestemmingsdialoogvenster duidelijk en ondubbelzinnig worden getoond,
- moet een bevestigende actie van de gebruiker vereisen (bijvoorbeeld tikken om te accepteren of een selectievakje aanvinken),
- mag het feit dat de gebruiker de kennisgeving verlaat (bijvoorbeeld door ergens anders te tikken of op de terug- of startknop te drukken) niet interpreteren als toestemming,
- mag niet gebruikmaken van berichten die automatisch worden gesloten of verlopen om zo toestemming te krijgen van de gebruiker, en
- moet worden ingewilligd door de gebruiker voordat de app kan beginnen met de verzameling van of toegang tot persoonsgegevens en gevoelige gebruikersgegevens.

Apps die een andere rechtsgrond gebruiken om persoonsgegevens en gevoelige gebruikersgegevens te verwerken zonder toestemming, zoals een legitiem belang op grond van de AVG van de Europese Unie, moeten voldoen aan alle toepasselijke wettelijke vereisten en passende kennisgevingen laten zien aan gebruikers, met inbegrip van kennisgevingen in de app zoals vereist op grond van dit beleid.

Om aan de beleidsvereisten te voldoen, raden we u aan de volgende voorbeeldindeling voor de prominente kennisgeving te bekijken als die vereist is:

- '[Deze app] verzamelt/verstuurt/synchroniseert/bewaart [type gegevens] om [functie] mogelijk te maken, [in welk scenario].'
- *Voorbeeld: 'Fitness Funds verzamelt locatiegegevens om fitness bij te kunnen houden, ook als de app gesloten is of niet wordt gebruikt. De gegevens worden ook gebruikt voor advertenties.'*
- *Voorbeeld: 'Call Buddy verzamelt lees- en schrijfgegevens voor logboeken om contacten te kunnen ordenen, ook als de app niet wordt gebruikt.'*

Als uw app code van derden (zoals een SDK) bevat die is ontworpen om standaard persoonsgegevens en gevoelige gebruikersgegevens te verzamelen, moet u binnen twee (2) weken na ontvangst van een verzoek van Google Play (of als in het verzoek van Google Play een langere periode is vermeld, binnen die periode) voldoende bewijs verstrekken waarin u aantoont dat uw app voldoet aan de vereisten voor prominente kennisgeving en toestemming van dit beleid, waaronder met betrekking tot de toegang tot gegevens en het verzamelen, gebruiken of delen ervan via de code van derden.

We hebben normen opgesteld die content definiëren en verbieden die schadelijk of ongepast is voor onze gebruikers om ervoor te zorgen dat Google Play een veilig en respectvol platform blijft.

- Een app die de apparaatlocatie verzamelt maar geen prominente kennisgeving heeft waarin wordt uitgelegd welke functie gebruikmaakt van deze gegevens en/of het gebruik van de app op de achtergrond wordt aangegeven.
- Een app die runtime-rechten heeft waarmee toegang tot gegevens wordt gevraagd voordat de prominente kennisgeving wordt getoond waarin wordt aangegeven waarvoor de gegevens worden gebruikt.
- Een app die toegang heeft tot een overzicht van de geïnstalleerde apps van een gebruiker en deze gegevens niet behandelt als persoonsgegevens of gevoelige gebruikersgegevens waarop de

bovenstaande vereisten voor het privacybeleid, de gegevensverwerking en de prominente kennisgeving en toestemming van toepassing zijn.

- Een app die toegang heeft tot de telefoonboek- of contactgegevens van een gebruiker en die deze gegevens niet behandelt als persoonsgegevens of gevoelige gebruikersgegevens waarop de bovenstaande vereisten voor het privacybeleid, de gegevensverwerking en de prominente kennisgeving en toestemming van toepassing zijn.
- Een app die het scherm van een gebruiker opneemt en deze gegevens niet als persoonsgegevens of gevoelige gebruikersgegevens behandelt op grond van dit beleid.
- Een app die de apparaatlocatie verzamelt, en het gebruik daarvan niet duidelijk bekendmaakt en toestemming verkrijgt in overeenstemming met de vereisten hiervoor.
- Een app die op de achtergrond van de app beperkte rechten gebruikt, bijvoorbeeld voor tracking-, onderzoeks- of marketingdoeleinden, en het gebruik ervan niet volledig openbaar maakt en geen toestemming krijgt in overeenstemming met de bovenstaande vereisten.
- Een app met een SDK die persoonsgegevens en gevoelige gebruikersgegevens verzamelt en deze gegevens niet behandelt overeenkomstig dit beleid voor gebruikersgegevens en de vereisten op het gebied van toegang, gegevensverwerking (met inbegrip van niet-toegestane verkoop), prominente kennisgeving en toestemming.

Lees dit artikel voor meer informatie over de vereisten voor prominente kennisgeving en toestemming.

**Beperkingen voor de toegang tot persoonsgegevens en gevoelige gegevens**

In aanvulling op de voorgaande vereisten worden in de tabel hierna de vereisten voor specifieke activiteiten beschreven.

| Activiteit | Vereiste |
|---|---|
| Uw app werkt met financiële of betalingsgegevens of nummers van door de overheid uitgegeven identiteitsbewijzen | De app mag persoonsgegevens en gevoelige gebruikersgegevens over financiële of betalingsactiviteiten of nummers van door de overheid uitgegeven identiteitsbewijzen nooit openbaar maken. |
| Uw app werkt met niet-openbare telefoonboek- of contactgegevens | We staan geen ongeautoriseerde publicatie of openbaarmaking van niet-openbare contactgegevens van mensen toe. |
| Uw app bevat een antivirus- of beveiligingsfunctie, zoals antivirus, antimalware of beveiligingsgerelateerde functies | Uw app moet een privacybeleid plaatsen dat, samen met kennisgevingen in de app, toelicht welke gebruikersgegevens door uw app worden verzameld en overgedragen, hoe deze gegevens worden gebruikt en met wie de gegevens worden gedeeld. |
| Uw app is gericht op kinderen | Uw app mag geen SDK bevatten die niet is goedgekeurd voor gebruik in op kinderen gerichte services. Zie Apps ontwerpen voor kinderen en gezinnen voor de volledige beleidsregels en eisen. |
| Uw app verzamelt of linkt naar permanente apparaat-ID's (zoals IMEI, IMSI, serienummer van de simkaart, enzovoort) | Permanente apparaat-ID's mogen niet worden gekoppeld aan andere persoonsgegevens en gevoelige gebruikersgegevens of apparaat-ID's die kunnen worden gereset, behalve ten behoeve van<br>• telefonie die is gekoppeld aan een sim-identiteit (bijvoorbeeld bellen via wifi koppelen aan het account van de provider), en<br>• zakelijke apps voor apparaatbeheer die de modus Apparaateigenaar gebruiken.<br>Dit gebruik moet duidelijk bekendgemaakt worden aan gebruikers, zoals vermeld in het Beleid voor gebruikersgegevens .<br>Raadpleeg deze bron voor alternatieve unieke ID's.<br>Lees het Advertentiebeleid voor aanvullend advies over de Android-advertentie-ID. |

### Gedeelte Veiligheid van gegevens

Alle ontwikkelaars moeten een duidelijk en nauwkeurig gedeelte Veiligheid van gegevens invullen voor elke app, waarin wordt vermeld hoe gebruikersgegevens worden verzameld, gebruikt en gedeeld. De ontwikkelaar is verantwoordelijk voor de nauwkeurigheid van het label en het actueel houden van deze informatie. Indien relevant moet het gedeelte Veiligheid van gegevens overeenstemmen met de kennisgevingen die zijn opgenomen in het privacybeleid van de app.

Bestudeer dit artikel voor meer informatie over hoe u het gedeelte Veiligheid van gegevens invult.

### Privacybeleid

Alle apps moeten een link naar het privacybeleid posten in het daarvoor bestemde veld in de Play Console en een link naar het privacybeleid of de tekst van het privacybeleid in de app zelf. Het privacybeleid moet, samen met eventuele kennisgevingen in de app, volledig openbaar maken hoe uw app gebruikersgegevens verzamelt, gebruikt, deelt en hiertoe toegang krijgt, niet beperkt tot de gegevens die worden bekendgemaakt in het gedeelte Veiligheid van gegevens. De volgende informatie moet worden vermeld:

- Informatie over de ontwikkelaar en een contactpersoon voor privacyzaken of een mechanisme om vragen te kunnen indienen.
- Bekendmaking van de soorten persoonsgegevens en gevoelige gebruikersgegevens waartoe uw app toegang heeft en die uw app verzamelt, gebruikt en deelt, en eventuele partijen waarmee deze gegevens worden gedeeld.
- Beveiligde procedures voor het werken met persoonsgegevens en gevoelige gebruikersgegevens.
- Het beleid van de ontwikkelaar voor de bewaring en verwijdering van gegevens.
- Duidelijke vermelding dat het een privacybeleid betreft (bijvoorbeeld aangemerkt als Privacybeleid in de titel).

De entiteit (zoals de ontwikkelaar of het bedrijf) die wordt genoemd in de Google Play Store-vermelding moet worden vermeld in het privacybeleid, of de app moet worden genoemd in het privacybeleid. Apps die geen toegang hebben tot persoonsgegevens en gevoelige gebruikersgegevens moeten toch een privacybeleid indienen.

Zorg dat uw privacybeleid beschikbaar is via een actieve en openbaar toegankelijke URL (geen pdf) die niet voorzien is van een geofence en dat deze niet kan worden bewerkt.

### Vereiste voor de verwijdering van accounts

Als uw app toestaat dat gebruikers een account maken in uw app, moet de app ook toestaan dat gebruikers hun account verwijderen. Gebruikers moeten beschikken over een makkelijk vindbare optie om de verwijdering van het app-account te starten in uw app. In het daarvoor bestemde URL-formulierveld in de Play Console moet daarvoor een link naar deze internethulpbron worden vermeld.

Als u een app-account op verzoek van een gebruiker verwijdert, moet u ook de aan het app-account gekoppelde gebruikersgegevens verwijderen. Het tijdelijk deactiveren, uitzetten of 'bevriezen' van het app-account wordt niet beschouwd als het verwijderen van het app-account. Als u bepaalde gegevens om legitieme redenen (zoals veiligheid, fraudebestrijding of naleving van regelgeving) moet bewaren, moet u gebruikers duidelijk informeren over uw praktijken met betrekking tot de bewaring van gegevens (bijvoorbeeld in uw privacybeleid).

Ga voor meer informatie over de beleidsvereisten voor de verwijdering van accounts naar dit Helpcentrum-artikel. Ga naar dit artikel voor meer informatie over het updaten van uw formulier Veiligheid van gegevens.

## Gebruik van app-set-ID

Android introduceert een nieuwe ID ter ondersteuning van essentiële toepassingen, zoals analyse en fraudepreventie. U vindt de gebruiksvoorwaarden voor deze ID hieronder.

- **Gebruik**: De app-set-ID moet niet worden gebruikt voor advertentiepersonalisatie en -metingen.
- **Koppeling aan persoonlijk identificeerbare informatie of andere ID's:** De app-set-ID mag niet worden gekoppeld aan Android-ID's (zoals AAID) of aan persoonsgegevens en gevoelige gegevens voor advertentiedoeleinden.
- **Transparantie en toestemming:** Het feit dat de app-set-ID wordt vastgelegd en gebruikt en dat u deze voorwaarden naleeft, moet openbaar worden gemaakt aan gebruikers in een privacymelding die voldoet aan de wettelijke vereisten, waaronder uw privacybeleid. Waar vereist moet u wettelijk geldige toestemming van gebruikers krijgen. Bekijk ons Beleid voor gebruikersgegevens voor meer informatie over onze privacynormen.

### EU-U.S. Privacy Shield (EU-VS privacyschild) en Swiss-U.S. Privacy Shield (Zwitserland-VS privacyschild)

Als u door Google beschikbaar gestelde persoonlijke informatie opent, gebruikt of verwerkt waarin een persoon direct of indirect wordt geïdentificeerd en die afkomstig is uit de Europese Unie of Zwitserland ('Persoonlijke informatie uit de EU'), is het volgende van toepassing:

- u moet voldoen aan alle toepasselijke wetgeving, richtlijnen, voorschriften en regels met betrekking tot privacy, gegevensbeveiliging en gegevensbescherming,
- u mag Persoonlijke informatie uit de EU alleen openen, gebruiken of verwerken voor doeleinden die overeenkomen met de toestemming die is verkregen van de persoon waarop de Persoonlijke informatie uit de EU betrekking heeft,
- u moet passende organisatorische en technische maatregelen implementeren om de Persoonlijke informatie uit de EU te beschermen tegen verlies, misbruik en ongeautoriseerde of onwettige toegang, kennisgeving, aanpassing en vernietiging,
- u moet hetzelfde beveiligingsniveau leveren als is vereist door de Privacy Shield-principes .

U moet regelmatig nagaan of u deze voorwaarden naleeft. Als u op enig moment niet aan deze voorwaarden kunt voldoen (of als er een aanzienlijk risico bestaat dat u er niet aan kunt voldoen), moet u ons onmiddellijk per e-mail informeren via data-protection-office@google.com en onmiddellijk stoppen met de verwerking van Persoonlijke informatie uit de EU of redelijke en passende maatregelen nemen om een toereikend beschermingsniveau te herstellen.

Sinds 16 juli 2020 maakt Google geen gebruik meer van het EU-U.S. Privacy Shield (EU-VS privacyschild) om persoonsgegevens vanuit de Europese Economische Ruimte of het Verenigd Koninkrijk door te geven aan de Verenigde Staten. (Meer informatie)Meer informatie vindt u in artikel 9 van de Distributieovereenkomst voor ontwikkelaars.

---

## Rechten en API's die toegang tot gevoelige informatie hebben

Gebruikers moeten verzoeken om rechten en API's die toegang tot gevoelige informatie hebben, kunnen begrijpen. U mag alleen om rechten en API's die toegang tot gevoelige informatie hebben, vragen die noodzakelijk zijn voor de implementatie van bestaande functies of services in uw app die worden gepromoot in uw Google Play-vermelding. U mag rechten of API's die toegang tot gevoelige informatie hebben en die toegang geven tot gebruikers- of apparaatgegevens niet gebruiken voor niet-bekendgemaakte, niet-uitgevoerde of niet-toegestane functies of doeleinden. Persoonsgegevens of gevoelige gebruikersgegevens waartoe toegang is verkregen door middel van rechten of API's die toegang hebben tot gevoelige informatie mogen nooit worden verkocht of gedeeld voor een doeleinde waarmee verkoop mogelijk is.

Vraag in context om rechten en API's die toegang tot gevoelige informatie hebben voor toegang tot gegevens (via incrementele verzoeken), zodat gebruikers begrijpen waarom uw app vraagt om die rechten. Gebruik de gegevens uitsluitend voor de doeleinden waarmee de gebruiker heeft ingestemd. Als u de gegevens later voor andere doeleinden wilt gebruiken, moet u dat aan gebruikers vragen en ervoor zorgen dat zij instemmen met het aanvullende gebruik.

**Beperkte rechten**

In aanvulling op het bovenstaande worden beperkte rechten omschreven als rechten die zijn geclassificeerd als Gevaarlijk , Speciaal , Handtekening of zoals hieronder beschreven. Op deze rechten zijn de volgende aanvullende vereisten en beperkingen van toepassing:

- Gebruikers- of apparaatgegevens waartoe toegang wordt verkregen via beperkte rechten, worden beschouwd als persoonsgegevens en gevoelige gebruikersgegevens. De vereisten in het Beleid voor gebruikersgegevens zijn van toepassing.
- Respecteer het besluit van een gebruiker als deze een verzoek om beperkte rechten afwijst. Gebruikers mogen ook niet worden gemanipuleerd of gedwongen om toestemming te geven voor niet-cruciale rechten. U moet voldoende alternatieven bieden om tegemoet te komen aan gebruikers die geen toegang verlenen tot gevoelige rechten (bijvoorbeeld de gebruiker toestaan handmatig een telefoonnummer in te toetsen als ze de toegang tot de gesprekslijsten hebben beperkt).
- Het gebruik van rechten in strijd met het malwarebeleid van Google Play (met inbegrip van misbruik van hogere rechten ) is uitdrukkelijk verboden.

Op bepaalde beperkte rechten kunnen de hieronder beschreven extra vereisten van toepassing zijn. Het doel van deze beperkingen is de waarborging van de privacy van de gebruiker. We kunnen beperkte uitzonderingen toestaan op de onderstaande vereisten in de zeldzame gevallen waarin apps een zeer aantrekkelijke of noodzakelijke functie bieden en waarbij momenteel geen alternatieve methode is om de functie aan te bieden. We beoordelen voorgestelde uitzonderingen op potentiële privacy- of beveiligingsgevolgen voor gebruikers.

## Rechten voor sms en gesprekslijsten

Sms en gesprekslijsten worden beschouwd als persoonlijke en gevoelige gebruikersgegevens waarop het beleid voor persoonlijke en gevoelige informatie en de volgende beperkingen van toepassing zijn:

| Beperkte rechten | Vereiste |
|---|---|
| **Rechtengroep Gesprekkenlijst (zoals READ_CALL_LOG, WRITE_CALL_LOG, PROCESS_OUTGOING_CALLS)** | De app moet actief worden geregistreerd als de standaard telefoon- of Assistent-handler op het apparaat. |
| **Rechtengroep Sms (zoals READ_SMS, SEND_SMS, WRITE_SMS, RECEIVE_SMS, RECEIVE_WAP_PUSH, RECEIVE_MMS)** | De app moet actief worden geregistreerd als de standaard sms- of Assistent-handler op het apparaat. |

Apps zonder standaard sms-, telefoon- of Assistent-handlermogelijkheden mogen het gebruik van de bovenstaande rechten niet definiëren in het manifest. Dit omvat tevens tekst in tijdelijke aanduidingen in het manifest. Daarnaast moeten apps actief worden geregistreerd als standaard sms-, telefoon- of Assistent-handler voordat gebruikers wordt gevraagd om een van de bovenstaande rechten te accepteren. De apps moeten onmiddellijk stoppen met het gebruik van de rechten als ze niet langer de standaardhandler zijn. De toegestane gebruiksmogelijkheden en uitzonderingen zijn beschikbaar op deze pagina van het Helpcentrum .

Apps mogen alleen de rechten (en eventuele gegevens die afkomstig zijn van deze rechten) gebruiken om goedgekeurde kernfunctionaliteit van de app te leveren. Kernfunctionaliteit wordt gedefinieerd als het belangrijkste doel van de app. Dit kan bestaan uit een reeks kernfuncties die alle duidelijk moeten worden beschreven en gepromoot in de beschrijving van de app. Zonder de kernfunctie(s) is de app 'defect' of wordt deze onbruikbaar. De overdracht, het delen of het gelicentieerde gebruik van deze gegevens mag uitsluitend plaatsvinden voor het verstrekken van kernfuncties of -services binnen de app en het gebruik ervan mag nooit worden uitgebreid tot eventuele andere doeleinden (zoals de verbetering van andere apps of services, reclame- of marketingdoeleinden). U mag geen alternatieve

methoden (waaronder andere rechten, API's of externe bronnen) gebruiken om gegevens te verkrijgen die zijn toegewezen aan rechten voor sms- en gesprekslijsten.

## Locatierechten

Apparaatlocatie wordt gezien als persoonsgegevens en gevoelige gebruikersgegevens waarop het Beleid voor persoonlijke en gevoelige informatie , het Beleid voor locatie op de achtergrond en de volgende vereisten van toepassing zijn:

- Apps mogen geen toegang krijgen tot gegevens die zijn beschermd door locatierechten (zoals ACCESS_FINE_LOCATION, ACCESS_COARSE_LOCATION, ACCESS_BACKGROUND_LOCATION) nadat dit niet langer noodzakelijk is om de betreffende functies of services in uw app te leveren.
- Verzoek nooit om locatierechten van gebruikers voor alleen advertentie- of analysedoeleinden. Apps die het toegestane gebruik van deze gegevens uitbreiden tot de weergave van advertenties, moeten voldoen aan ons Advertentiebeleid .
- Apps moeten om het minimale verzoeken (bijvoorbeeld geschat in plaats van gedetailleerd of voorgrond in plaats van achtergrond) om de betreffende functie of service te bieden waarvoor de locatie vereist is. Gebruikers moeten redelijkerwijs kunnen verwachten dat de functie of service het locatieniveau nodig heeft waarom wordt verzocht. We kunnen bijvoorbeeld apps afwijzen die zonder overtuigende motivering verzoeken om achtergrondlocatie.
- De locatie op de achtergrond mag alleen worden gebruikt om functies te bieden die nuttig zijn voor de gebruiker en relevant zijn voor de kernfunctionaliteit van de app.

Apps mogen toegang tot de locatie via de service op de voorgrond hebben (als de app alleen voorgrondtoegang heeft, bijvoorbeeld 'tijdens gebruik') als het gebruik:

- is gestart als een voortzetting van een door de gebruiker gestarte actie in de app, en
- meteen wordt beëindigd nadat de beoogde toepassing van de door de gebruiker gestarte actie is voltooid door de app.

Apps die specifiek zijn ontworpen voor kinderen, moeten voldoen aan het beleid voor Gemaakt voor gezinnen .

Bekijk dit Help-artikel voor meer informatie over de beleidsvereisten.

## Rechten voor toegang tot alle bestanden

Bestanden en directorykenmerken op het apparaat van een gebruiker worden beschouwd als persoonlijke en gevoelige gebruikersgegevens waarop het beleid voor persoonlijke en gevoelige gegevens en de volgende vereisten van toepassing zijn:

- Apps mogen alleen toegang vragen tot apparaatopslag die essentieel is voor de werking van de app en mogen geen toegang vragen tot apparaatopslag namens derden voor doeleinden die geen verband houden met kritieke, op de gebruiker gerichte app-functionaliteit.
- Android-apparaten met R of hoger hebben het recht MANAGE_EXTERNAL_STORAGE nodig om toegang in gedeelde opslag te beheren. Alle apps die R targeten en brede toegang tot gedeelde opslag vragen ('Toegang tot alle bestanden'), moeten een juiste toegangscontrole doorlopen voordat ze kunnen worden gepubliceerd. Apps die dit recht mogen gebruiken, moeten gebruikers duidelijk vragen 'Toegang tot alle bestanden' in te schakelen voor hun app onder de instellingen voor 'Speciale app-toegang'. Bekijk dit Help-artikel voor meer informatie over de R-vereisten.

## Rechten voor pakket-/app-zichtbaarheid

De voorraad van geïnstalleerde apps die vanaf een apparaat wordt opgevraagd, wordt beschouwd als persoonlijke en gevoelige gebruikersgegevens waarop het beleid voor persoonlijke en gevoelige informatie en de volgende vereisten van toepassing zijn:

Apps die als kerndoel hebben om andere apps op het apparaat te starten, te zoeken of ermee samen te werken, kunnen mogelijk voor het bereik geschikte zichtbaarheid krijgen voor andere geïnstalleerde apps op het apparaat, zoals hieronder beschreven:

- **Brede app-zichtbaarheid**: Brede zichtbaarheid is het vermogen van een app om uitgebreide (brede) zichtbaarheid te krijgen voor de geïnstalleerde apps (pakketten) op een apparaat.
  - Voor apps die API-niveau 30 of hoger targeten, is brede zichtbaarheid voor geïnstalleerde apps via het recht QUERY_ALL_PACKAGES beperkt tot specifieke toepassingen waarbij bekendheid en/of interoperabiliteit met alle apps op het apparaat nodig is voor de werking van de app.
    - U mag QUERY_ALL_PACKAGES niet gebruiken als uw app kan werken met een meer gerichte, voor het bereik geschikte definitie voor pakketzichtbaarheid (bijvoorbeeld zoeken naar en interactie hebben met specifieke pakketten in plaats van brede zichtbaarheid aanvragen).
  - Het gebruik van alternatieve methoden om het brede zichtbaarheidsniveau te benaderen dat hoort bij het recht QUERY_ALL_PACKAGES, is ook beperkt tot de op de gebruiker gerichte kernfunctionaliteit van de app en interoperabiliteit met apps die via deze methode worden ontdekt.
  - Bekijk dit Helpcentrum-artikel voor toegestane toepassingen van het recht QUERY_ALL_PACKAGES.
- **Beperkte app-zichtbaarheid**: Van beperkte zichtbaarheid is sprake wanneer een app de toegang tot gegevens beperkt door naar specifieke apps te zoeken via meer gerichte (in plaats van brede) methoden (bijvoorbeeld door te zoeken naar specifieke apps die voldoen aan de manifestverklaring van uw app). U kunt deze methode gebruiken om te zoeken naar apps als uw app beschikt over beleidsconforme interoperabiliteit of beheer van deze apps.
- De zichtbaarheid van de voorraad van geïnstalleerde apps op een apparaat moet rechtstreeks verband houden met het kerndoel of de kernfunctionaliteit waartoe gebruikers toegang hebben in uw app.

App-voorraadgegevens die worden opgevraagd via op Play gedistribueerde apps, mogen nooit worden verkocht of gedeeld voor analysedoeleinden of om inkomsten te genereren met advertenties.

## API voor toegankelijkheid

De API voor toegankelijkheid mag niet worden gebruikt:

- om de instellingen van gebruikers te wijzigen zonder hun toestemming of te voorkomen dat gebruikers een app of service kunnen uitzetten of verwijderen, tenzij geautoriseerd door een ouder of voogd via een app voor ouderlijk toezicht of door gemachtigde beheerders via zakelijke beheersoftware,
- om de ingebouwde privacyopties en -meldingen van Android te omzeilen, of
- om de gebruikersinterface te wijzigen of te gebruiken op een manier die misleidend is of anderszins in strijd is met het Beleid voor ontwikkelaars van Google Play.

De API voor toegankelijkheid is niet ontworpen en mag niet worden aangevraagd voor externe gespreksaudio-opnamen.

Het gebruik van de API voor toegankelijkheid moet worden gedocumenteerd in de Google Play-vermelding.

### Richtlijnen voor IsAccessibilityTool

Apps met een kernfunctionaliteit die bedoeld is om mensen met beperkingen rechtstreeks te ondersteunen, komen in aanmerking voor het gebruik van **IsAccessibilityTool** om zichzelf publiekelijk aan te merken als toegankelijkheidsapp.

Apps die niet in aanmerking komen voor **IsAccessibilityTool**, mogen het label niet gebruiken en moeten voldoen aan de vereisten voor prominente kennisgeving en toestemming zoals uiteengezet in het Beleid voor gebruikersgegevens, aangezien de aan toegankelijkheid gerelateerde functionaliteit

niet duidelijk is voor de gebruiker. Bekijk het Helpcentrum-artikel over de AccessibilityService API voor meer informatie.

Apps moeten waar mogelijk API's en rechten met een beperkter bereik gebruiken in plaats van de API voor toegankelijkheid om de gewenste functionaliteit mogelijk te maken.

**Het recht Request_Install_Packages (Installatiepakketten aanvragen)**

Met het recht REQUEST_INSTALL_PACKAGES kan een app om de installatie van app-pakketten verzoeken. Om dit recht te gebruiken, moet uw app de volgende kernfunctionaliteit hebben:

- app-pakketten versturen of ontvangen, en
- door de gebruiker gestarte installatie van app-pakketten mogelijk maken.

Toegestane functies zijn onder meer:

- Browsen op internet of zoeken
- Communicatieservices die bijlagen ondersteunen
- Bestanden delen, overdragen of beheren
- Zakelijk apparaatbeheer
- Back-up maken en terugzetten
- Apparaatmigratie/telefoonoverdracht
- Begeleidende app om telefoon te synchroniseren met wearable of IoT-apparaat (bijvoorbeeld smartwatch of smart-tv)

De kernfunctionaliteit is het hoofddoel van de app. De kernfunctionaliteit, plus eventuele kernfuncties waaruit deze kernfunctionaliteit bestaat, moeten allemaal duidelijk worden beschreven en gepromoot in de beschrijving van de app.

Het recht REQUEST_INSTALL_PACKAGES mag niet worden gebruikt om zelf-updates of wijzigingen uit te voeren, of andere APK's te bundelen in het itembestand, tenzij dit is bedoeld voor apparaatbeheer. Alle updates en de installatie van pakketten moeten voldoen aan het Beleid tegen misbruik van apparaten en netwerken van Google Play en moeten worden gestart en uitgevoerd door de gebruiker.

**Rechten voor Health Connect van Android**

Gegevens waartoe toegang wordt verkregen via de rechten voor Health Connect worden beschouwd als persoonsgegevens en gevoelige gebruikersgegevens waarop het beleid voor gebruikersgegevens van toepassing is, evenals de volgende aanvullende vereisten:

**Juiste toegang tot en gebruik van Health Connect**

Verzoeken om toegang tot gegevens via Health Connect moeten duidelijk en begrijpelijk zijn. Health Connect mag alleen worden gebruikt in overeenstemming met de toepasselijke beleidsregels en algemene voorwaarden, en alleen voor goedgekeurde toepassingen, zoals beschreven in dit beleid. Dit houdt in dat u alleen om toegang tot rechten mag vragen als uw app of service voldoet aan een van de goedgekeurde toepassingen.

Goedgekeurde toepassingen voor toegang tot de rechten voor Health Connect zijn:

- Apps of services met een of meer functies die de gezondheid en fitness van de gebruiker ten goede komen via een gebruikersinterface waarmee gebruikers rechtstreeks hun fysieke activiteiten, slaap, mentale welzijn, voeding, gezondheidsmetingen, fysieke beschrijvingen en/of andere gezondheids- of fitnessgerelateerde beschrijvingen en metingen kunnen **bijhouden, vastleggen, monitoren en/of analyseren**.
- Apps of services met een of meer functies die de gezondheid en fitness van de gebruiker ten goede komen via een gebruikersinterface waarmee gebruikers rechtstreeks hun fysieke activiteiten, slaap, mentale welzijn, voeding, gezondheidsmetingen, fysieke beschrijvingen en/of andere gezondheids- of fitnessgerelateerde beschrijvingen en metingen kunnen **opslaan** op hun telefoon en/of wearable,

en hun gegevens kunnen delen met andere apps op het apparaat die voldoen aan deze toepassingen.

Health Connect is een algemeen platform voor het opslaan en delen van gegevens waarmee gebruikers gezondheids- en fitnessgegevens kunnen verzamelen uit verschillende bronnen op hun Android-apparaat en deze naar keuze kunnen delen met derden. De gegevens kunnen afkomstig zijn uit verschillende bronnen, zoals vastgesteld door de gebruikers. Ontwikkelaars moeten beoordelen of Health Connect geschikt is voor het beoogde gebruik en de bron en kwaliteit van gegevens afkomstig uit Health Connect onderzoeken en valideren in verband met een doel en, in het bijzonder, voor gebruik in het kader van onderzoek, gezondheid en medische toepassingen.

- Apps die gezondheidsgerelateerd onderzoek met menselijke proefpersonen uitvoeren met behulp van gegevens die zijn verkregen via Health Connect moeten toestemming krijgen van deelnemers of, in geval van minderjarigen, hun ouder of voogd. In deze toestemming moet het volgende zijn vermeld: (a) aard, doel en duur van het onderzoek, (b) procedures, risico's en voordelen voor de deelnemers, (c) informatie over de vertrouwelijkheid en verwerking van gegevens (waaronder eventueel delen met derden), (d) een contactpersoon voor vragen van deelnemers, en (e) de herroepingsprocedure. Apps die gezondheidsgerelateerd onderzoek met menselijke proefpersonen uitvoeren met behulp van gegevens die zijn verkregen via Health Connect moeten goedkeuring verkrijgen van een onafhankelijke raad die 1) als doel heeft de rechten, de veiligheid en het welzijn van de deelnemers te beschermen en 2) beschikt over de bevoegdheid om onderzoek met menselijke proefpersonen te verifiëren, aan te passen en goed te keuren. Op verzoek moet het bewijs van dergelijke goedkeuring worden overgelegd.
- Het is ook uw verantwoordelijkheid om ervoor te zorgen dat eventuele wet- en regelgeving die van toepassing kan zijn op uw beoogde gebruik van Health Connect en gegevens afkomstig uit Health Connect wordt nageleefd. Behalve voor zover uitdrukkelijk is vermeld op de labels of informatie die door Google wordt verstrekt voor specifieke Google-producten of -services, keurt Google het gebruik van in Health Connect beschikbare gegevens niet goed voor enig gebruik of enig doeleinde, en, in het bijzonder in het kader van onderzoek, gezondheid of medische toepassingen. Google garandeert evenmin de juistheid van de in Health Connect beschikbare gegevens voor het voorgaande. Google wijst alle aansprakelijkheid af die samenhangt met het gebruik van gegevens die zijn verkregen via Health Connect.

**Beperkt gebruik**

Als Health Connect wordt gebruikt voor een geschikt doel, moet uw gebruik van de gegevens die zijn verkregen via Health Connect ook voldoen aan de onderstaande vereisten. Deze vereisten zijn van toepassing op de onbewerkte gegevens die zijn verkregen via Health Connect en op gegevens die zijn verzameld of geanonimiseerd op basis van of afgeleid van de onbewerkte gegevens.

- Beperk uw gebruik van Health Connect-gegevens tot het verstrekken of verbeteren van uw geschikte toepassing of functies die zichtbaar en prominent aanwezig zijn in de gebruikersinterface van de verzoekende app.
- Draag gebruikersgegevens uitsluitend over aan derden:
  - voor het verstrekken of verbeteren van uw geschikte toepassing of functies die duidelijk zijn op grond van de gebruikersinterface van de verzoekende app en uitsluitend met toestemming van de gebruiker,
  - indien noodzakelijk voor beveiligingsdoeleinden (bijvoorbeeld voor het onderzoeken van misbruik),
  - om te voldoen aan toepasselijke wet- en/of regelgeving, of
  - als onderdeel van een fusie, verwerving of verkoop van activa van de ontwikkelaar, na vooraf uitdrukkelijke toestemming te hebben verkregen van de gebruiker.
- Sta mensen niet toe de gebruikersgegevens te lezen, tenzij:
  - de uitdrukkelijke toestemming is verkregen van de gebruiker om specifieke gegevens te lezen,
  - dit noodzakelijk is voor beveiligingsdoeleinden (bijvoorbeeld voor het onderzoeken van misbruik),

- om te voldoen aan toepasselijke wetgeving, of
- de gegevens (met inbegrip van afgeleide gegevens) worden verzameld en gebruikt voor interne processen in overeenstemming met het toepasselijke privacybeleid en andere wettelijke voorschriften in die jurisdictie.

Alle andere overdracht, gebruik of verkoop van Health Connect-gegevens is verboden, met inbegrip van:

- de overdracht of verkoop van gebruikersgegevens aan derden, zoals advertentieplatforms, gegevensmakelaars of andere resellers van informatie,
- de overdracht, de verkoop of het gebruik van gebruikersgegevens voor het weergeven van advertenties, waaronder gepersonaliseerde of op interesses gebaseerde advertenties,
- de overdracht, de verkoop of het gebruik van gebruikersgegevens voor het vaststellen van de kredietwaardigheid of ten behoeve van leningen,
- de overdracht, de verkoop of het gebruik van de gebruikersgegevens met een product dat of service die kan worden beschouwd als medisch hulpmiddel overeenkomstig artikel 201(h) van de Amerikaanse Federal Food Drug & Cosmetic Act als de gebruikersgegevens worden gebruikt door het medische hulpmiddel om zijn gereguleerde functie uit te voeren,
- de overdracht, de verkoop of het gebruik van gebruikersgegevens voor een doeleinde of op een wijze waarbij beveiligde medische gegevens (Protected Health Information, PHI) zoals gedefinieerd in de Amerikaanse HIPAA betrokken zijn, tenzij u vooraf schriftelijke goedkeuring krijgt voor dergelijk gebruik van Google.

De toegang tot Health Connect mag niet worden gebruikt op een manier die dit beleid of andere toepasselijke algemene voorwaarden of beleidsregels voor Health Connect schendt, waaronder voor de volgende doeleinden:

- Gebruik Health Connect niet bij de ontwikkeling van, of voor de opname in, apps, omgevingen of activiteiten waarbij bij het gebruik van of een storing in Health Connect redelijkerwijs kan worden verwacht dat dit leidt tot overlijden, persoonlijk letsel of schade aan het milieu of eigendommen (zoals de bouw of werking van kernfaciliteiten, luchtverkeersleiding, levensinstandhoudingssystemen of wapens).
- Verkrijg geen toegang tot gegevens die zijn verkregen via Health Connect met behulp van apps zonder interface. Apps moeten een duidelijk herkenbaar icoon in het app-vak, app-instellingen op het apparaat, meldingsiconen enzovoort, weergeven.
- Gebruik Health Connect niet met apps die gegevens synchroniseren tussen niet-compatibele apparaten of platforms.
- Health Connect mag geen verbinding maken met apps, services of functies die zich uitsluitend op kinderen richten. Health Connect is niet goedgekeurd voor gebruik in primair op kinderen gerichte services.

Een verklaring waarin wordt bevestigd dat uw gebruik van Health Connect-gegevens voldoet aan de vereisten ten aanzien van het beperkte gebruik moet worden verstrekt in uw app of op een website die behoort tot uw webservice of app, zoals een link op een homepage of in het privacybeleid waarin het volgende staat: 'Het gebruik van gegevens die worden verkregen uit Health Connect voldoet aan het beleid ten aanzien van rechten voor Health Connect, met inbegrip van de vereisten ten aanzien van beperkt gebruik.'

**Minimaal bereik**

U mag alleen om toegang tot rechten verzoeken die van cruciaal belang zijn voor de uitvoering van de functies van uw app of service.

Dit betekent het volgende:

- Vraag niet om informatie die u niet nodig heeft. Vraag alleen om toegang tot rechten die noodzakelijk zijn om de functies of services van uw product uit te voeren. Als uw product geen

toegang vereist tot specifieke rechten, mag u niet verzoeken om toegang tot deze rechten.

**Transparente en nauwkeurige kennisgeving en controle**

Health Connect verwerkt gezondheids- en fitnessgegevens, waaronder persoonlijke en gevoelige informatie. Alle apps en services moeten een privacybeleid bevatten, waarin uitgebreid moet worden vermeld hoe uw app of service gebruikersgegevens verzamelt, gebruikt en deelt. Dit omvat onder meer de soorten partijen waarmee gebruikersgegevens worden gedeeld, de manier waarop u de gegevens gebruikt, hoe u de gegevens opslaat en beveiligt en wat er gebeurt met de gegevens als een account wordt gedeactiveerd en/of verwijderd.

In aanvulling op de vereisten op grond van de toepasselijke wetgeving, moet u ook aan de volgende vereisten voldoen:

- U moet een kennisgeving verstrekken over de verzameling, het gebruik en het delen van gegevens. Deze kennisgeving:
  - moet op correcte wijze de identiteit van de app of service weergeven die toegang wil verkrijgen tot gebruikersgegevens,
  - moet duidelijke en correcte informatie verstrekken waarin wordt toegelicht welke soorten gegevens worden bekeken, verkregen en/of verzameld,
  - moet een toelichting bevatten over de manier waarop de gegevens worden gebruikt en/of gedeeld. Als u gegevens verzamelt voor het ene doeleinde, maar de gegevens ook gebruikt worden voor een secundair doeleinde, moet u gebruikers informeren over beide toepassingen.
- U moet helpdocumentatie voor gebruikers verstrekken waarin wordt toegelicht hoe gebruikers hun gegevens in uw app kunnen beheren of deze kunnen verwijderen.

**Beveiligde gegevensverwerking**

Alle gebruikersgegevens moeten op beveiligde wijze worden verwerkt. Neem redelijke en passende stappen om alle apps of systemen die gebruikmaken van Health Connect te beschermen tegen onbevoegd(e) of onrechtmatig(e) toegang, gebruik, vernietiging, verlies, wijziging of openbaarmaking.

Aanbevolen beveiligingspraktijken bestaan onder meer uit de invoering en het onderhouden van een managementsysteem voor informatiebeveiliging, zoals beschreven in ISO/IEC 27001 en de waarborging dat uw app of webservice robuust is en vrij van veelvoorkomende beveiligingsproblemen, zoals beschreven in de OWASP Top 10.

Afhankelijk van de API waartoe toegang wordt verkregen en het aantal gebruikersverleningen of gebruikers, vereisen wij dat uw app of service een periodieke beveiligingsbeoordeling ondergaat en dat u een beoordelingsbrief verkrijgt van een aangewezen derde als uw product gegevens overdraagt buiten het eigen apparaat van de gebruiker.

Meer informatie over vereisten voor apps die verbinding maken met Health Connect vindt u in dit Help-artikel.

**VPNService**

De VpnService is een basisklasse voor apps om hun eigen VPN-oplossingen uit te breiden en te ontwerpen. Alleen apps die de VpnService gebruiken en waarvan VPN de kernfunctionaliteit is, kunnen op apparaatniveau een beveiligde tunnel maken naar een server op afstand. Uitzonderingen zijn onder meer apps die een server op afstand vereisen voor kernfunctionaliteit, zoals:

- Apps voor ouderlijk toezicht en zakelijk beheer.
- Tracking van het app-gebruik.
- Apps voor apparaatveiligheid (zoals antivirus, beheer van mobiele apparaten, firewall).
- Netwerkgerelateerde tools (zoals toegang op afstand).
- Apps voor het browsen op internet.

- Apps van providers die het gebruik van VPN-functionaliteit vereisen om telefonie- of connectiviteitsservices te leveren.

De VpnService kan niet worden gebruikt om:

- persoonsgegevens en gevoelige gebruikersgegevens te verzamelen zonder prominente kennisgeving en toestemming,
- gebruikersverkeer vanuit andere apps om te leiden of te manipuleren op een apparaat ten behoeve van het genereren van inkomsten (zoals het omleiden van advertentieverkeer via een ander land dan het land van de gebruiker),

Apps die de VpnService gebruiken:

- moeten het gebruik van de VpnService opgeven in de Google Play-vermelding, en
- moeten de gegevens van het apparaat tot het eindpunt van de VPN-tunnel versleutelen, en
- moeten zich houden aan het volledige Programmabeleid voor ontwikkelaars , waaronder het beleid voor Advertentiefraude , Rechten en Malware .

**Recht voor Exact alarm**

Er wordt een nieuw recht (USE_EXACT_ALARM) ingevoerd dat toegang biedt tot de functie Exact alarm in apps vanaf Android 13 (API-doelniveau 33).

USE_EXACT_ALARM is een beperkt recht en apps mogen dit recht alleen opgeven als de kernfunctionaliteit de noodzaak van een exact alarm ondersteunt. Apps die verzoeken om dit beperkte recht worden daarop beoordeeld en als niet wordt voldaan aan de criteria voor acceptabele gebruikstoepassingen, wordt de app niet gepubliceerd op Google Play.

**Acceptabele gebruikstoepassingen voor het gebruik van het exacte alarm**

Uw app mag de functie USE_EXACT_ALARM alleen gebruiken als de tot de gebruiker gerichte kernfunctionaliteit van uw app acties met een precieze tijdsaanduiding vereisen, zoals:

- de app is een wekker- of timer-app,
- de app is een kalender-app die gebeurtenismeldingen weergeeft.

Als u een gebruikstoepassing heeft voor de functie 'Exact alarm' die niet onder de hiervoor vermelde opties valt, moet u nagaan of u SCHEDULE_EXACT_ALARM kunt gebruiken als alternatieve optie.

Raadpleeg deze richtlijnen voor ontwikkelaars voor meer informatie over de functie Exact alarm.

---

## Apparaat- en netwerkmisbruik

We staan geen apps toe die het apparaat van de gebruiker, andere apparaten of computers, servers, netwerken, Application Programming Interfaces (API's) of services, met inbegrip van, maar niet beperkt tot andere apps op het apparaat, een Google-service of het netwerk van een erkende provider, verstoren, onderbreken, beschadigen of daartoe op onbevoegde wijze toegang verkrijgen.

Apps op Google Play moeten voldoen aan de standaardvereisten voor systeemoptimalisatie van Android die zijn vastgelegd in de richtlijnen voor core app-kwaliteit (Core App Quality Guidelines) voor Google Play .

Een app die wordt gedistribueerd via Google Play, mag zichzelf niet aanpassen, vervangen of updaten via een andere methode dan het updatemechanisme van Google Play. Ook mag een app geen uitvoerbare code (zoals dex-, jar- of so-bestanden) downloaden via een andere bron dan Google Play. Deze beperking geldt niet voor code die wordt uitgevoerd op een virtuele machine of een interpreter die indirecte toegang biedt tot Android-API's (zoals JavaScript in een WebView of browser).

Apps of code van derden (zoals SDK's) met geïnterpreteerde talen (JavaScript, Python, Lua, enzovoort) die tijdens de runtime zijn geladen (bijv. niet verpakt bij de app), mogen geen potentiële

schendingen van het Google Play-beleid toestaan.

We staan geen code toe die kwetsbaarheden in de beveiliging introduceert of misbruikt. Raadpleeg het Programma voor de verbetering van de beveiliging van apps voor meer informatie over de meest recente beveiligingsproblemen die zijn gemarkeerd voor ontwikkelaars.

We hebben normen opgesteld die content definiëren en verbieden die schadelijk of ongepast is voor onze gebruikers om ervoor te zorgen dat Google Play een veilig en respectvol platform blijft.

- Apps die de weergave van advertenties in een andere app verstoren of blokkeren.
- Cheat-apps die de gameplay van andere apps beïnvloeden.
- Apps met instructies voor het hacken van services, software of hardware, of die beveiligingsmaatregelen omzeilen.
- Apps die toegang krijgen tot een service of API of deze gebruiken op een manier die de servicevoorwaarden ervan schendt.
- Apps die niet in aanmerking komen voor opname op de witte lijst en die proberen het energiebeheer van het systeem te omzeilen,
- Apps die proxyservices naar derden mogelijk maken, mogen dat alleen doen in apps waar dat het primaire, op gebruikers gerichte doel van de app is,
- Apps of code van derden (bijvoorbeeld SDK's die uitvoerbare code (zoals DEX-bestanden of native code) downloaden via een andere bron dan Google Play.
- Apps die andere apps installeren op een apparaat zonder voorafgaande toestemming van de gebruiker.
- Apps die een link bevatten naar kwaadwillende software of de distributie of installatie daarvan mogelijk maken.
- Apps of code van derden (bijvoorbeeld SDK's) die een WebView met toegevoegde JavaScript-interface bevatten die niet-vertrouwde webcontent laadt (bijvoorbeeld een URL met http://) of niet-geverifieerde URL's die zijn verkregen via niet-vertrouwde bronnen (bijv. URL's die zijn verkregen via niet-vertrouwde intenties).

**Gebruik van services op de voorgrond**

Het recht Service op de voorgrond zorgt dat op gebruikers gerichte services op de voorgrond juist worden gebruikt. Als apps Android 14 of nieuwer targeten, geeft u een geldig type op voor elke service op de voorgrond die in uw app wordt gebruikt. Definieer ook het juiste recht voor services op de voorgrond voor dat type. Als voor de use case van uw app bijvoorbeeld de geolocatie voor een kaart is vereist, definieert u het recht FOREGROUND_SERVICE_LOCATION in uw app-manifest.

Met uitzondering van de typen services op de voorgrond systemExempted en shortService mag voor apps alleen een recht voor services op de voorgrond worden gedefinieerd als het gebruik hiervan:

- een functie aanbiedt die nuttig is voor de gebruiker en relevant is voor de kernfunctionaliteit van de app,
- wordt gestart door de gebruiker of door de gebruiker kan worden opgemerkt (bijvoorbeeld de audio van een nummer dat wordt afgespeeld, media die naar een ander apparaat wordt gecast, een duidelijke en nauwkeurige gebruikersmelding, een verzoek van een gebruiker om een foto te uploaden naar de cloud),
- kan worden gestopt door de gebruiker,
- kan niet worden onderbroken of uitgesteld door het systeem zonder dat dit leidt tot een negatieve gebruikerservaring of zorgt dat de door de gebruiker verwachte functie niet werkt zoals verwacht (een telefoongesprek moet bijvoorbeeld meteen starten en kan niet worden uitgesteld door het systeem),
- alleen wordt uitgevoerd zolang dit nodig is om de taak af te ronden.

Hier vindt u meer informatie over het gebruik van services op de voorgrond.

### Door de gebruiker gestarte gegevensoverdrachtstaken

Apps mogen alleen gebruikmaken van de API voor door de gebruiker gestarte gegevensoverdrachtstaken als het gebruik:

- is gestart door de gebruiker,
- bedoeld is voor gegevensoverdrachtstaken via het netwerk,
- alleen wordt uitgevoerd zolang dit nodig is om de gegevensoverdracht af te ronden.

Hier vindt u meer informatie over het gebruik van de API voor door de gebruiker gestarte gegevensoverdrachten.

### Vereisten aan de markering FLAG_SECURE

FLAG_SECURE is een flag die in de code van een app wordt opgegeven om aan te geven dat de UI gevoelige gegevens bevat die moeten worden beperkt tot een beveiligde omgeving tijdens het gebruik van de app. Deze flag is ontworpen om te voorkomen dat de gegevens worden weergegeven in screenshots of op niet-beveiligde schermen. Ontwikkelaars geven deze flag op wanneer de content van de app niet mag worden uitgezonden, bekeken of anderszins overgedragen buiten de app of het apparaat van de gebruiker.

Uit veiligheids- en privacyoverwegingen moeten alle apps die worden gedistribueerd op Google Play zich houden aan de definitie FLAG_SECURE van andere apps. Dit houdt in dat het niet is toegestaan voor apps om de FLAG_SECURE-instellingen in andere apps te omzeilen of hier de mogelijkheid toe te bieden.

Apps die worden aangemerkt als een toegankelijkheidstool zijn vrijgesteld van deze vereiste, mits ze geen door middel van FLAG_SECURE beschermde content sturen of (in het cachegeheugen) opslaan voor toegang buiten het apparaat van de gebruiker.

### Apps die Android-containers op het apparaat uitvoeren

Apps met Android-containers op het apparaat bieden omgevingen die een onderliggend Android OS geheel of gedeeltelijk simuleren. De functionaliteit binnen deze omgevingen komt misschien niet overeen met de volledige suite van Android-beveiligingsfuncties. Daarom kunnen ontwikkelaars ervoor kiezen een manifest-flag voor een beveiligde omgeving toe te voegen om aan Android-containers op het apparaat door te geven dat ze niet mogen worden uitgevoerd in hun gesimuleerde Android-omgeving.

### Manifest-flag voor beveiligde omgeving

REQUIRE_SECURE_ENV is een flag die kan worden gedefinieerd in het manifest van een app om aan te geven dat deze app niet moet worden uitgevoerd in apps met Android-containers op het apparaat. Uit veiligheids- en privacyoverwegingen moeten apps die Android-containers op het apparaat bieden, alle apps respecteren waarvoor deze flag is gedefinieerd en:

- De manifesten van apps die ze in hun Android-container op het apparaat willen laden, controleren op deze flag.
- De apps waarvoor deze flag is gedefinieerd, niet laden in hun Android-container op het apparaat.
- Niet fungeren als proxy door API's te onderscheppen of aan te roepen op het apparaat zodat geïnstalleerd lijken in de container.
- Omzeiling van de flag niet mogelijk maken en geen tijdelijke oplossingen daarvoor aanbieden (zoals een oudere versie van een app laden om de flag REQUIRE_SECURE_ENV van de huidige app te omzeilen).

Meer informatie over dit beleid vindt u in ons Helpcentrum.

---

## Misleidend gedrag

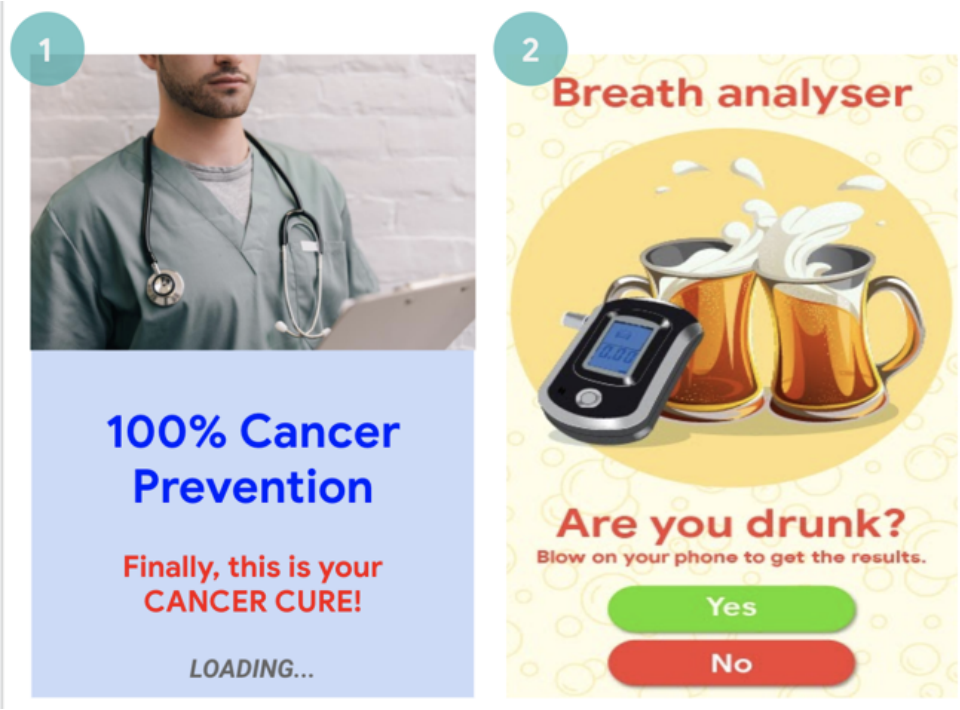
We staan geen apps toe die gebruikers proberen te misleiden of oneerlijk gedrag mogelijk maken, waaronder, maar niet beperkt tot, apps waarvan is bepaald dat ze functioneel onmogelijk zijn. Apps moeten een nauwkeurige kennisgeving, beschrijving en afbeeldingen/video van hun functionaliteit verstrekken in alle onderdelen van de metadata. Apps mogen geen functies of waarschuwingen nabootsen van het besturingssysteem of van andere apps. Wijzigingen in de apparaatinstellingen moeten worden doorgevoerd met medeweten en toestemming van de gebruiker en door de gebruiker ongedaan kunnen worden gemaakt.

## Misleidende claims

We staan geen apps toe die onjuiste of misleidende informatie bevatten, waaronder in de beschrijving, de titel, het icoon en screenshots.

We hebben normen opgesteld die content definiëren en verbieden die schadelijk of ongepast is voor onze gebruikers om ervoor te zorgen dat Google Play een veilig en respectvol platform blijft.

- Onduidelijke of onjuiste beschrijving van de functionaliteit van apps:
  - Een app die stelt een racegame te zijn in de beschrijving en screenshots, maar in feite een puzzelgame is waarbij een afbeelding van een auto wordt gebruikt.
  - Een app die stelt een antivirus-app te zijn, maar slechts een handleiding bevat met informatie over het verwijderen van virussen.
- Apps die stellen te beschikken over functies die niet uitgevoerd kunnen worden (zoals apps voor de bestrijding van insecten), ook niet als het duidelijk is dat het gaat om een grap, nep, enzovoort.
- Apps die onjuist zijn gecategoriseerd, inclusief maar niet beperkt tot de app-classificatie of app-categorie.
- Aantoonbaar misleidende of onjuiste content die stemprocessen kan verstoren, of over verkiezingsresultaten.
- Apps die ten onrechte beweren gelieerd te zijn aan een overheidsentiteit, of dat ze overheidsdiensten bieden of ondersteunen waarvoor ze niet geautoriseerd zijn.
- Apps die ten onrechte beweren de officiële app van een gevestigde entiteit te zijn. Een titel als Justin Bieber Official is niet toegestaan zonder de noodzakelijke toestemming of rechten.




(1) Deze app bevat medische of gezondheidsgerelateerde beweringen (genezing van kanker) die misleidend zijn.

(2) Deze apps stellen te beschikken over functies die niet kunnen worden uitgevoerd (bijvoorbeeld uw telefoon gebruiken als blaastest).

## Misleidende wijzigingen in de apparaatinstellingen

We staan geen apps toe die zonder medeweten en toestemming van de gebruiker wijzigingen aanbrengen in de apparaatinstellingen van de gebruiker of in functies van andere apps. Apparaatinstellingen en functies omvatten tevens systeem- en browserinstellingen, bookmarks, sneltoetsen, iconen, widgets en de weergave van apps op het startscherm.

Daarnaast staan we ook het volgende niet toe:

- Apps die de apparaatinstellingen of functies wijzigen met toestemming van de gebruiker, maar dat zodanig doen dat de wijziging niet eenvoudig ongedaan gemaakt kan worden.
- Apps of advertenties die apparaatinstellingen of functies wijzigen als service aan derden of ten behoeve van advertenties.
- Apps die gebruikers misleiden om apps van derden te verwijderen of uit te schakelen of om apparaatinstellingen of functies te wijzigen.
- Apps die gebruikers aansporen of aanmoedigen om apps van derden te verwijderen of uit te schakelen of om apparaatinstellingen of functies te wijzigen, tenzij dit deel uitmaakt van een verifieerbare beveiligingsservice.

## Oneerlijk gedrag mogelijk maken

We staan geen apps toe waarmee gebruikers anderen kunnen misleiden of die functioneel op welke manier dan ook misleidend zijn, inclusief maar niet beperkt tot apps die identiteitsdocumenten, burgerservicenummers, paspoorten, diploma's, creditcards, bankrekeningen en rijbewijzen genereren of dit mogelijk maken. Apps moeten voorzien in nauwkeurige kennisgevingen, titels, beschrijvingen en afbeeldingen/video over de functies en/of content van de app. Ze moeten ook op de juiste manier presteren zoals de gebruiker redelijkerwijs kan verwachten.

Aanvullende app-bronnen (zoals game-items) mogen alleen worden gedownload als ze noodzakelijk zijn voor het gebruik van de app door de gebruiker. Gedownloade resources moeten voldoen aan alle beleidsregels van Google Play en voordat de download wordt gestart, moet de app dit melden aan gebruikers en duidelijk de grootte van de download aangeven.

De mededeling dat een app een 'grapje' is of 'bestemd voor amusementsdoeleinden' (of soortgelijke bewoordingen) stelt een app niet vrij van de toepassing van onze beleidsregels.

We hebben normen opgesteld die content definiëren en verbieden die schadelijk of ongepast is voor onze gebruikers om ervoor te zorgen dat Google Play een veilig en respectvol platform blijft.

- Apps die andere apps of websites nabootsen zodat gebruikers worden misleid om hun persoonlijke en verificatiegegevens bekend te maken.
- Apps die niet-geverifieerde of echte telefoonnummers, contacten, adressen of persoonlijke identificeerbare informatie weergeven of afbeelden van individuen of entiteiten die hiervoor geen toestemming hebben verleend.
- Apps met verschillende kernfunctionaliteit op basis van de geografie, apparaatparameters of andere gebruikersafhankelijke gegevens van een gebruiker waarbij deze verschillen niet prominent aan de gebruiker worden getoond in de winkelvermelding.
- Apps die aanzienlijk wijzigingen aanbrengen tussen versies zonder de gebruiker te waarschuwen (bijvoorbeeld in het gedeelte 'Wat is er nieuw' ) en de winkelvermelding te updaten.
- Apps die proberen hun gedrag tijdens de beoordeling aan te passen of te obfusceren.
- Apps met door content delivery network (CDN) ondersteunde downloads die geen melding geven aan de gebruiker en de grootte van de download niet bekendmaken voorafgaand aan de download.

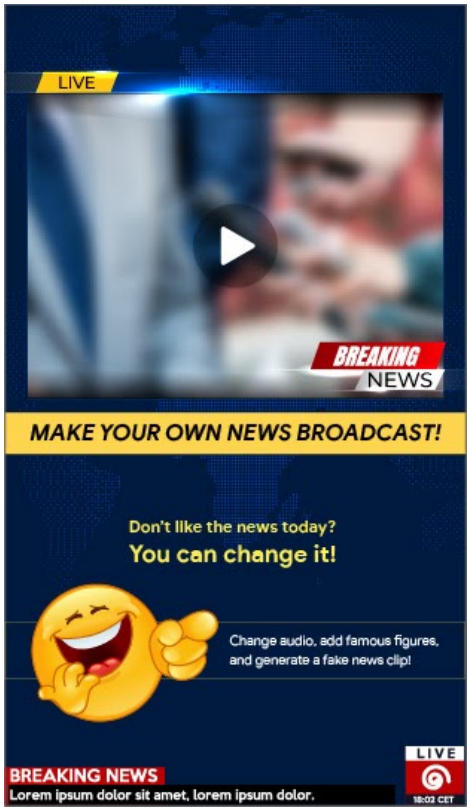
## Gemanipuleerde media

We staan geen apps toe die onjuiste of misleidende informatie of claims promoten of helpen maken die worden overgebracht via afbeeldingen, video's en/of tekst. We staan geen apps toe waarvan is vastgesteld dat ze aantoonbaar misleidende of bedrieglijke afbeeldingen, video's en/of tekst bevatten of verspreiden en die schade kunnen toebrengen aan een gevoelig evenement, de politiek, sociale kwesties of andere zaken van publiek belang.

Apps die media manipuleren of wijzigen, als dat verder gaat dan gebruikelijke en redactioneel aanvaardbare aanpassingen voor duidelijkheid of kwaliteit, moeten gewijzigde media als zodanig bekendmaken of watermerken als het voor de doorsnee persoon mogelijk niet duidelijk is dat de media is gewijzigd. Er kunnen uitzonderingen worden gemaakt voor het publieke belang of voor een duidelijke satire of parodie.

We hebben normen opgesteld die content definiëren en verbieden die schadelijk of ongepast is voor onze gebruikers om ervoor te zorgen dat Google Play een veilig en respectvol platform blijft.

- apps die een publiek figuur toevoegen aan een demonstratie tijdens een politiek gevoelig evenement;
- apps die publieke figuren of media van een gevoelig evenement gebruiken om de mogelijkheden om media te wijzigen te promoten in de winkelvermelding van een app;
- apps die mediaclips wijzigen om een nieuwsuitzending te imiteren.




(1) Deze app biedt functionaliteit om mediaclips te wijzigen om een nieuwsuitzending na te bootsen en zonder watermerk beroemde of openbare personen aan de clip toe te voegen.

**Transparantie van gedrag**

De functionaliteit van uw app moet redelijk duidelijk zijn voor gebruikers. Neem geen verborgen, inactieve of niet-gedocumenteerde functies op in uw app. Technieken om app-beoordelingen te omzeilen zijn niet toegestaan. Voor apps moet misschien aanvullende informatie worden verstrekt om de veiligheid van gebruikers, de integriteit van het systeem en de naleving van het beleid te waarborgen.

---

## Verkeerde voorstelling

We staan geen apps of ontwikkelaarsaccounts toe die:

- zich valselijk voordoen als personen of organisaties, of die een verkeerde voorstelling geven van hun eigenaarschap of primaire doel of deze aspecten verhullen.
- zich bezighouden met onechte of gecoördineerde activiteiten om gebruikers te misleiden. Dit omvat, maar is niet beperkt tot, apps of ontwikkelaarsaccounts die een verkeerde voorstelling geven van hun land van herkomst of dit verbergen en die content weergeven aan gebruikers in een ander land.
- samenwerken met andere apps, sites, ontwikkelaars of andere accounts om de details van ontwikkelaars of apps of andere belangrijke details te verbergen of hier een verkeerde voorstelling van te geven als de app-content betrekking heeft op politiek, maatschappelijke kwesties of kwesties van algemeen belang.

---

## Beleid voor doel-API-niveau van Google Play

We willen gebruikers veilige en betrouwbare functionaliteit bieden. Daarom vereist Google Play de volgende API-niveaus voor **alle apps**:

**Nieuwe apps en app-updates MOETEN** een Android API-niveau targeten dat binnen één jaar van de nieuwste grote Android-versierelease valt. Voor nieuwe apps en app-updates die niet aan deze vereiste voldoen, is app-inzending in de Play Console niet mogelijk.

**Bestaande Google Play-apps die niet worden geüpdatet** en die geen API-niveau targeten dat binnen 2 jaar van de nieuwste grote Android-versierelease valt, zijn niet beschikbaar voor nieuwe gebruikers met apparaten waarop een nieuwere versie van Android OS is geïnstalleerd. Gebruikers die de app eerder hebben geïnstalleerd via Google Play, kunnen de app nog steeds vinden, opnieuw installeren en gebruiken op elke Android OS-versie die de app ondersteunt.

Bekijk de migratiehandleiding voor technisch advies om te voldoen aan de vereiste voor het doel-API-niveau.

Ga naar dit Helpcentrum-artikel voor de exacte tijdlijnen en uitzonderingen.

---

## SDK-vereisten

App-ontwikkelaars maken vaak gebruik van code van derden (zoals een SDK) om belangrijke functionaliteit en services in hun apps te integreren. Als u een SDK in uw app opneemt, moet u zorgen dat u uw gebruikers en de app kunt beschermen tegen eventuele kwetsbaarheden. Dit artikel gaat over hoe sommige van onze bestaande privacy- en beveiligingsvereisten van toepassing zijn op SDK's en hoe deze vereisten ontworpen zijn om ontwikkelaars te helpen SDK's veilig en beveiligd te integreren in hun apps.

Als u een SDK in uw app opneemt, is het uw verantwoordelijkheid om te zorgen dat uw app met de code en de praktijken van derden niet het Programmabeleid voor ontwikkelaars van Google Play schendt. Het is belangrijk om te weten hoe de SDK's in uw app met gebruikersgegevens omgaan. Zorg daarom dat u weet welke rechten ze gebruiken, welke gegevens ze verzamelen en waarom. De verzameling en verwerking van gebruikersgegevens door een SDK moet afgestemd zijn op het gebruik van die gegevens in overeenstemming met het beleid van uw app.

Lees en begrijp het volledige beleid hieronder om te zorgen dat uw gebruik van een SDK de beleidsvereisten niet schendt. Let vooral op de daarin genoemde vereisten specifiek voor SDK's.

### Beleid voor gebruikersgegevens

U moet transparant zijn over hoe u omgaat met gebruikersgegevens (zoals gegevens die van of over een gebruiker verzameld worden, waaronder apparaatgegevens). Dit betekent dat u bekendmaakt of en hoe er toegang wordt gekregen tot gebruikersgegevens in uw app, en hoe deze worden verzameld, gebruikt, verwerkt en gedeeld. Het betekent ook dat u het gebruik van de gegevens beperkt tot de bekendgemaakte en beleidsconforme doeleinden.

Als u code van derden (zoals een SDK) in uw app opneemt, moet u zorgen dat deze code aan het Programmabeleid voor ontwikkelaars van Google Play voldoet. Ook moet alle omgang van deze derde partij met de gebruikersgegevens uit uw app daaraan voldoen. Dit programmabeleid bestaat onder meer uit gebruiks- en kennisgevingsvereisten. U moet bijvoorbeeld zorgen dat uw SDK-providers geen persoonsgegevens en gevoelige gebruikersgegevens uit uw app verkopen. Deze vereiste geldt ongeacht of gebruikersgegevens nu worden overgedragen nadat ze naar een server zijn gestuurd, of door het insluiten van de code van derden in uw app.

### Persoonsgegevens en gevoelige gebruikersgegevens

- Beperk de toegang, het verzamelen, het gebruik en het delen van persoonsgegevens en gevoelige gebruikersgegevens verkregen via de app, tot de app- en servicefuncties en beleidsconforme doeleinden die de gebruiker redelijkerwijs kan verwachten:
  - Apps die het gebruik van persoonsgegevens en gevoelige gebruikersgegevens uitbreiden voor de weergave van advertenties, moeten voldoen aan het Advertentiebeleid van Google Play.
- Zorg dat u beveiligd werkt met alle persoonsgegevens en gevoelige gebruikersgegevens, inclusief het overdragen van de gegevens met behulp van moderne versleuteling (bijvoorbeeld via https).
- Gebruik waar mogelijk een verzoek om runtimerechten voordat toegang wordt verkregen tot gegevens die worden afgeschermd door Android-rechten.

### Verkoop van persoonsgegevens en gevoelige gebruikersgegevens

U mag geen persoonsgegevens of gevoelige gebruikersgegevens verkopen.

- Onder 'verkoop' wordt verstaan: De uitwisseling of overdracht van persoonsgegevens en gevoelige gebruikersgegevens aan een derde voor een geldelijke vergoeding.
  - Een door de gebruiker gestarte overdracht van persoonsgegevens en gevoelige gebruikersgegevens wordt niet beschouwd als verkoop (bijvoorbeeld als de gebruiker een functie in de app gebruikt om een bestand over te dragen aan een derde of als de gebruiker ervoor kiest een specifieke app te gebruiken voor speciale onderzoeksdoeleinden).

### Vereisten voor prominente kennisgeving en toestemming

Als de toegang van uw app tot persoonsgegevens en gevoelige gebruikersgegevens of het verzamelen, gebruiken of delen ervan niet binnen de redelijke verwachting van de gebruiker van het betreffende product of de betreffende functie valt, moet u voldoen aan de vereiste voor prominente kennisgeving en toestemming van het Beleid voor gebruikersgegevens.

Als uw app code van derden (zoals een SDK) bevat die ontworpen is om standaard persoonsgegevens en gevoelige gebruikersgegevens te verzamelen, moet u binnen twee (2) weken na ontvangst van een verzoek van Google Play (of als in het verzoek van Google Play een langere periode is vermeld, binnen die periode) voldoende bewijs verstrekken waarin u aantoont dat uw app voldoet aan de vereisten voor prominente kennisgeving en toestemming van dit beleid, waaronder met betrekking tot de toegang tot gegevens en het verzamelen, gebruiken of delen ervan via de code van derden.

Zorg dat uw app door het gebruik van code van derden (zoals een SDK) niet het Beleid voor gebruikersgegevens schendt.

Raadpleeg dit Helpcentrum-artikel voor meer informatie over de vereiste voor prominente kennisgeving en toestemming.

### Voorbeelden van door SDK veroorzaakte schendingen:

- Een app met een SDK die persoonsgegevens en gevoelige gebruikersgegevens verzamelt en deze gegevens niet behandelt overeenkomstig dit Beleid voor gebruikersgegevens en de vereisten op het gebied van toegang, gegevensverwerking (met inbegrip van niet-toegestane verkoop), prominente kennisgeving en toestemming.
- Een app integreert een SDK die standaard persoonsgegevens en gevoelige gebruikersgegevens verzamelt, in strijd met de vereisten van dit beleid voor toestemming van gebruikers en prominente kennisgeving.
- Een app met een SDK die claimt alleen persoonsgegevens en gevoelige gebruikersgegevens te verzamelen om antifraude- en antimisbruikfunctionaliteit voor de app te bieden, maar de verzamelde gegevens ook met derden deelt voor advertentie- of analysedoeleinden.
- Een app gebruikt een SDK die informatie over geïnstalleerde pakketten van gebruikers verstuurt zonder te voldoen aan de richtlijnen voor prominente kennisgeving en/of de privacybeleidsrichtlijnen.

- Raadpleeg ook het Beleid voor ongewenste mobiele software.

### Aanvullende vereisten voor toegang tot gevoelige en persoonsgegevens

De tabel hierna beschrijft de vereisten voor specifieke activiteiten.

| Activiteit | Vereiste |
| --- | --- |
| Uw app verzamelt of linkt naar permanente apparaat-ID's (zoals IMEI, IMSI, serienummer van de simkaart, enzovoort) | Permanente apparaat-ID's mogen niet worden gekoppeld aan andere persoonsgegevens of gevoelige gebruikersgegevens of aan apparaat-ID's die kunnen worden gereset, behalve ten behoeve van:<br>• telefonie die gekoppeld is aan een sim-identiteit (bijvoorbeeld bellen via wifi koppelen aan het account van de provider), en<br>• zakelijke apps voor apparaatbeheer die de modus Apparaateigenaar gebruiken.<br>Dit gebruik moet duidelijk bekendgemaakt worden aan gebruikers, zoals vermeld in het Beleid voor gebruikersgegevens .<br>Raadpleeg deze bron voor alternatieve unieke ID's.<br>Lees het Advertentiebeleid voor aanvullend advies over de Android-advertentie-ID. |
| Uw app is gericht op kinderen | Uw app mag alleen SDK's gebruiken die zelfgecertificeerd zijn voor op kinderen gerichte services. Raadpleeg het Programma voor zelfgecertificeerde advertentie-SDK's voor gezinnen voor de volledige beschrijving en vereisten van het beleid. |

### Voorbeelden van door SDK veroorzaakte schendingen:

- Een app gebruikt een SDK die de Android-ID aan Locatie koppelt.
- Een app met een SDK die de AAID aan permanente apparaat-ID's koppelt voor advertentie- of analysedoeleinden.
- Een app gebruikt een SDK die de AAID aan het e-mailadres koppelt voor analysedoeleinden.

### Gedeelte Veiligheid van gegevens

Alle ontwikkelaars moeten een duidelijk en nauwkeurig gedeelte Veiligheid van gegevens invullen voor elke app, waarin wordt vermeld hoe gebruikersgegevens worden verzameld, gebruikt en gedeeld. Dit geldt ook voor gegevens die worden verzameld en verwerkt via bibliotheken of SDK's van derden die in hun apps worden gebruikt. De ontwikkelaar is verantwoordelijk voor de nauwkeurigheid van het label en het actueel houden van deze informatie. Waar relevant moet het gedeelte Veiligheid van gegevens overeenstemmen met de kennisgevingen die opgenomen zijn in het privacybeleid van de app.

Raadpleeg dit Helpcentrum-artikel voor meer informatie over hoe u het gedeelte Veiligheid van gegevens invult.

Zie het volledige Beleid voor gebruikersgegevens.

## Beleid voor rechten en API's die toegang tot gevoelige informatie hebben

Gebruikers moeten verzoeken om rechten en API's die toegang tot gevoelige informatie hebben, kunnen begrijpen. U mag alleen vragen om rechten en API's die toegang tot gevoelige informatie hebben als dit noodzakelijk is voor de implementatie van bestaande functies of services in uw app die worden gepromoot in uw Google Play-vermelding. U mag rechten of API's met toegang tot gevoelige informatie en gebruikers- of tot apparaatgegevens niet gebruiken voor niet-bekendgemaakte, niet-uitgevoerde of niet-toegestane functies of doeleinden. Persoonsgegevens of gevoelige gebruikersgegevens waartoe toegang is verkregen door middel van rechten of API's die toegang hebben tot gevoelige informatie mogen nooit worden verkocht of gedeeld voor een doeleinde waarmee verkoop mogelijk is.

Zie het volledige Beleid voor rechten en API's die toegang hebben tot gevoelige informatie.

**Voorbeelden van door SDK veroorzaakte schendingen:**

- Uw app bevat een SDK die op de achtergrond locatie opvraagt voor een niet-toegestaan of niet-openbaar gemaakt doel.
- Uw app bevat een SDK die zonder toestemming van de gebruiker de IMEI verzendt die is afgeleid van het Android-recht read_phone_state.

## Malwarebeleid

Ons malwarebeleid is simpel: het Android-ecosysteem (inclusief de Google Play Store) en apparaten van gebruikers moeten vrij zijn van schadelijk gedrag (d.w.z. malware). Met behulp van dit fundamentele beginsel streven we ernaar om een beveiligd Android-ecosysteem te bieden voor onze gebruikers en hun Android-apparaten.

Malware is elke code die een gebruiker, de gegevens van een gebruiker of een apparaat in gevaar brengt. Malware omvat, maar is niet beperkt tot, potentieel schadelijke apps (Potentially Harmful Applications, PHA), binaire bestanden of frameworkaanpassingen die vallen binnen categorieën zoals Trojaanse paarden, phishing en spyware-apps. We updaten deze lijst voortdurend en voegen nieuwe categorieën toe.

Zie het volledige Malwarebeleid.

**Voorbeelden van door SDK veroorzaakte schendingen:**

- Een app die het rechtenmodel van Android schendt of inloggegevens (zoals OAuth-tokens) steelt uit andere apps.
- Apps die functies misbruiken om te voorkomen dat de apps worden verwijderd of gestopt.
- Een app die SELinux uitzet.
- Uw app gebruikt een SDK die het rechtenmodel van Android schendt door rechten op een hoger niveau te verkrijgen via de toegang tot apparaatgegevens voor een niet bekendgemaakt doel.
- Uw app bevat een SDK met code die gebruikers ertoe verleidt zich te abonneren of content te kopen via hun mobiele telefoonrekening.

Apps die zich rechten toe-eigenen en apparaten rooten zonder toestemming van de gebruiker, worden geclassificeerd als root-apps.

## Beleid voor ongewenste mobiele software

### Transparant gedrag en duidelijke openbaarmakingen

Alle code moet beloften waarmaken die aan de gebruiker zijn gedaan. Apps moeten alle meegedeelde functionaliteit bieden. Apps mogen gebruikers niet in verwarring brengen.

**Voorbeelden van schendingen:**

- Advertentiefraude
- Social engineering

### Beschermen van gebruikersgegevens

Wees duidelijk en transparant over de toegang, het gebruik, het verzamelen en het delen van persoonsgegevens en gevoelige gebruikersgegevens. Het gebruik van gebruikersgegevens moet voldoen aan alle relevante Beleidsregels voor gebruikersgegevens, indien van toepassing, en alle voorzorgsmaatregelen nemen om de gegevens te beschermen.

**Voorbeelden van schendingen:**

- Gegevensverzameling (vergelijk: Spyware)
- Misbruik van beperkte rechten

Zie het volledige Beleid voor ongewenste mobiele software

## Beleid voor apparaat- en netwerkmisbruik

We staan geen apps toe die het apparaat van de gebruiker, andere apparaten of computers, servers, netwerken, Application Programming Interfaces (API's) of services, inclusief maar niet beperkt tot andere apps op het apparaat, een Google-service of het netwerk van een erkende provider, verstoren, onderbreken, beschadigen of er op onbevoegde wijze toegang toe verkrijgen.

Apps of code van derden (zoals SDK's) met geïnterpreteerde talen (JavaScript, Python, Lua, enzovoort) die tijdens de runtime geladen zijn (bijv. niet verpakt bij de app), mogen geen potentiële schendingen van het Google Play-beleid toestaan.

We staan geen code toe die kwetsbaarheden in de beveiliging introduceert of misbruikt. Raadpleeg het Programma voor de verbetering van de beveiliging van apps voor meer informatie over de meest recente beveiligingsproblemen die zijn gemarkeerd voor ontwikkelaars.

Zie het volledige Beleid voor apparaat- en netwerkmisbruik.

**Voorbeelden van door SDK veroorzaakte schendingen:**

- Apps die proxyservices aan derden mogelijk maken, mogen dat alleen doen in apps waar dat het primaire, op gebruikers gerichte doel van de app is.
- Uw app bevat een SDK die uitvoerbare code downloadt, zoals dex-bestanden of native code, van een andere bron dan Google Play.
- Uw app bevat een SDK die een WebView met toegevoegde JavaScript-interface bevatten die niet-vertrouwde webcontent laadt (bijvoorbeeld een URL met http://) of niet-geverifieerde URL's die zijn verkregen via niet-vertrouwde bronnen (bijv. URL's die zijn verkregen via niet-vertrouwde intenties).
- Uw app bevat een SDK met code die wordt gebruikt voor het updaten van de eigen APK
- Uw app bevat een SDK die gebruikers blootstelt aan een beveiligingslek door bestanden te downloaden via een niet-beveiligde verbinding.
- Uw app gebruikt een SDK met code om apps van onbekende bronnen buiten Google Play om te downloaden of te installeren.

**Beleid tegen misleidend gedrag**

We staan geen apps toe die gebruikers proberen te misleiden of oneerlijk gedrag mogelijk maken, inclusief maar niet beperkt tot apps waarvan is bepaald dat ze functioneel onmogelijk zijn. Apps moeten in alle onderdelen van de metadata een nauwkeurige kennisgeving, beschrijving en afbeeldingen/video van hun functionaliteit verstrekken. Apps mogen geen functies of waarschuwingen nabootsen van het besturingssysteem of van andere apps. Wijzigingen in de apparaatinstellingen moeten worden doorgevoerd met medeweten en toestemming van de gebruiker en door de gebruiker ongedaan kunnen worden gemaakt.

Zie het volledige Beleid tegen misleidend gedrag.

**Transparantie van gedrag**

De functionaliteit van uw app moet redelijk duidelijk zijn voor gebruikers. Neem geen verborgen, inactieve of niet-gedocumenteerde functies op in uw app. Technieken om app-beoordelingen te omzeilen zijn niet toegestaan. Voor apps moet misschien aanvullende informatie worden verstrekt om de veiligheid van gebruikers, de integriteit van het systeem en de naleving van het beleid te waarborgen.

**Voorbeeld van een door een SDK veroorzaakte schending**

- Uw app bevat een SDK die technieken gebruikt om app-beoordelingen te omzeilen.

**Welk beleid voor ontwikkelaars van Google Play wordt vaak in verband gebracht met door SDK veroorzaakte schendingen?**

Raadpleeg de volgende beleidsregels in hun geheel om ervoor te zorgen dat alle code van derden die uw app gebruikt, voldoet aan het Programmabeleid voor ontwikkelaars van Google Play:

- Beleid voor gebruikersgegevens
- Rechten en API's met toegang tot gevoelige informatie
- Beleid voor apparaat- en netwerkmisbruik
- Malware
- Ongewenste mobiele software
- Programma voor zelfgecertificeerde advertentie-SDK's voor gezinnen
- Advertentiebeleid
- Misleidend gedrag
- Programmabeleid voor ontwikkelaars van Google Play

Hoewel deze beleidsregels over het algemeen vaker worden geschonden, is het belangrijk om te onthouden dat uw app door slechte SDK-code een beleid kan schenden dat hierboven niet wordt genoemd. Vergeet vooral niet om alle beleidsregels in hun geheel door te nemen en up-to-date te blijven van alle beleidsregels. Het is uw verantwoordelijkheid als app-ontwikkelaar om te zorgen dat uw SDK's beleidsconform met uw app-gegevens omgaan.

Ga voor meer informatie naar ons Helpcentrum.

---

## Malware

Ons malwarebeleid is simpel: het Android-ecosysteem, inclusief de Google Play Store, en apparaten van gebruikers moeten vrij zijn van kwaadwillend gedrag (d.w.z. malware). Met behulp van dit fundamentele beginsel streven we ernaar om een beveiligd Android-ecosysteem te bieden voor onze gebruikers en hun Android-apparaten.

Malware is elke code die een gebruiker, de gegevens van een gebruiker of een apparaat in gevaar brengt. Malware omvat, maar is niet beperkt tot, potentieel schadelijke apps (Potentially Harmful Applications, PHA), binaire bestanden of frameworkaanpassingen, bestaande uit categorieën zoals Trojaanse paarden, phishing en spyware-apps. We updaten deze lijst voortdurend door nieuwe categorieën toe te voegen.

Hoewel er verschillende typen malware zijn met verschillende mogelijkheden, heeft malware meestal een van de volgende doelen:

- De integriteit van het apparaat van de gebruiker in gevaar brengen.
- De controle verkrijgen over het apparaat van een gebruiker.
- Activiteiten op afstand mogelijk maken waardoor een aanvaller toegang krijgt tot een besmet apparaat of dit kan gebruiken of op een andere manier kan exploiteren.
- Persoonsgegevens of andere gegevens van het apparaat halen zonder toereikende kennisgeving of toestemming.
- Spam of opdrachten verspreiden vanaf het besmette apparaat naar andere apparaten of netwerken.
- De gebruiker oplichten.

Een app, binair bestand of frameworkaanpassing kan potentieel schadelijk zijn, en dus kwaadwillend gedrag genereren, zelfs als het niet de bedoeling was om schadelijk te zijn. Dit komt omdat apps, binaire bestanden of frameworkaanpassingen verschillend kunnen functioneren, afhankelijk van allerlei variabelen. Oftewel: iets wat schadelijk is voor het ene Android-apparaat, hoeft geen risico te vormen voor een ander Android-apparaat. Een apparaat waarop bijvoorbeeld de nieuwste versie van Android wordt uitgevoerd, heeft geen last van schadelijke apps die gebruikmaken van beëindigde API's om schadelijk gedrag uit te voeren. Een apparaat waarop nog een zeer vroege versie van Android wordt uitgevoerd, kan echter risico lopen. Apps, binaire bestanden of frameworkaanpassingen worden

gemarkeerd als malware of PHA als ze duidelijk een risico vormen voor sommige of alle Android-apparaten en gebruikers.

De onderstaande malwarecategorieën weerspiegelen onze fundamentele overtuiging dat gebruikers moeten begrijpen hoe hun apparaat kan worden gebruikt of misbruikt. Ze promoten ook een beveiligd ecosysteem dat robuuste innovatie en een vertrouwde gebruikerservaring mogelijk maakt.

Ga naar Google Play Protect voor meer informatie.

## Backdoors

Code waarmee ongewenste, potentieel schadelijke bewerkingen op afstand kunnen worden uitgevoerd op een apparaat.

Deze bewerkingen kunnen onder meer bestaan uit gedrag waardoor de app, het binaire bestand of de frameworkaanpassing in een van de andere malwarecategorieën kan worden geplaatst als het automatisch wordt uitgevoerd. 'Backdoor' (achterdeur) is een algemene beschrijving van de manier waarop potentieel schadelijke bewerkingen kunnen worden uitgevoerd op een apparaat. Daarom komt dit niet volledig overeen met categorieën als factureringsfraude of commerciële spyware. Als gevolg daarvan kan een subset van dergelijke backdoors onder bepaalde omstandigheden door Google Play Protect worden behandeld als een kwetsbaarheid.

## Factureringsfraude

Code waarmee op een opzettelijk misleidende manier automatisch kosten in rekening worden gebracht aan de gebruiker.

Telecomfraude wordt opgesplitst in sms-fraude, belfraude en betaal-/abonneerfraude.

*Sms-fraude*
Code die kosten in rekening brengt aan gebruikers om zonder toestemming premium sms-berichten te sturen of die probeert de bijbehorende sms-activiteiten te verhullen door kennisgevingsovereenkomsten of sms-berichten van de mobiele provider te verbergen waarin de gebruiker op de hoogte wordt gesteld van kosten of waarin abonnementen worden bevestigd.

Bepaalde code (hoewel deze technisch gezien het gedrag met betrekking tot het sturen van sms-berichten bekend maakt) introduceert aanvullend gedrag dat sms-fraude mogelijk maakt. Voorbeelden omvatten het verbergen of onleesbaar maken van delen van een kennisgevingsovereenkomst voor de gebruiker of het voorwaardelijk onderdrukken van sms-berichten van de mobiele provider waarin de gebruiker op de hoogte wordt gesteld van kosten of waarin een abonnement wordt bevestigd.

*Belfraude*
Code waarmee kosten in rekening worden gebracht aan gebruikers door premium nummers te bellen zonder toestemming van de gebruiker.

*Betaal-/abonneerfraude*
Code die gebruikers misleidt zodat ze zich abonneren of content kopen via hun mobiele telefoonrekening.

Betaal-/abonneerfraude omvat elk type facturering, met uitzondering van premium sms-berichten en premium gesprekken. Voorbeelden hiervan omvatten rechtstreekse facturering via provider, draadloze toegangspunten (WAP) en overdracht van mobiele zendtijd. WAP-fraude is een van de meest voorkomende typen betaal-/abonneerfraude. WAP-fraude kan gebruikers misleiden zodat ze op een knop klikken in een transparante WebView die onzichtbaar is geladen. Als de gebruiker de actie uitvoert, wordt een abonnement gestart dat steeds wordt verlengd. De sms of e-mail ter bevestiging wordt vaak onderschept om te voorkomen dat gebruikers de financiële transactie opmerken.

## Stalkerware

Code die persoonsgegevens of gevoelige gebruikersgegevens verzamelt van een apparaat en deze gegevens verstuurt naar een derde (bedrijf of andere persoon) om die gebruiker te volgen.

Apps moeten een voldoende prominente kennisgeving verstrekken en toestemming verkrijgen zoals vereist in het Beleid voor gebruikersgegevens .

**Richtlijnen voor volg-apps**

Apps die exclusief zijn ontworpen en in de handel worden gebracht om een andere persoon te volgen, bijvoorbeeld ouders die hun kinderen in de gaten willen houden of ten behoeve van ondernemingsbeheer om afzonderlijke medewerkers te volgen, zijn de enige toegestane volg-apps, mits ze volledig voldoen aan de onderstaande vereisten. Deze apps mogen niet worden gebruikt om iemand anders (bijvoorbeeld een echtgenoot/echtgenote) in de gaten te houden, zelfs niet met medeweten en toestemming van de betreffende persoon, ongeacht of er een permanente melding wordt weergegeven. Deze apps moeten de metadatamarkering IsMonitoringTool in hun manifestbestand gebruiken om zichzelf naar behoren aan te duiden als volg-app.

Volg-apps moeten voldoen aan deze vereisten:

- Apps mogen zich niet presenteren als een spionage-oplossing of als oplossing voor geheim toezicht.
- Apps mogen geen trackinggedrag verbergen of verhullen of gebruikers proberen te misleiden over dergelijke functies.
- Apps moeten gebruikers een permanente melding laten zien als de app actief is, evenals een uniek icoon waarmee de app duidelijk kan worden geïdentificeerd.
- Apps moeten de monitorings- of volgfunctie bekendmaken in de beschrijving in de Google Play Store.
- Apps en app-vermeldingen op Google Play mogen geen middelen bieden om functies te activeren of toegankelijk te maken die deze voorwaarden schenden, zoals een link naar een ongeschikte APK die buiten Google Play wordt gehost.
- Apps moeten voldoen aan alle toepasselijke wetgeving. U bent als enige verantwoordelijk voor het bepalen van de wettigheid van uw app in het getargete land.

Bekijk het Helpcentrum-artikel Gebruik van de markering isMonitoringTool voor meer informatie.

## Denial of Service (DoS)

Code die, zonder medeweten van de gebruiker, een DoS-aanval (Denial of Service) uitvoert of deel uitmaakt van een gedistribueerde DoS-aanval tegen andere systemen en bronnen.

Dit kan bijvoorbeeld worden gedaan door een groot aantal HTTP-verzoeken te sturen om overmatige belasting op externe servers te produceren.

## Schadelijke downloaders

Code die zelf niet schadelijk is, maar andere PHA's downloadt.

In de volgende gevallen kan code een schadelijke downloader zijn:

- Er is reden om aan te nemen dat de code is gemaakt om PHA's te verspreiden en de code heeft PHA's gedownload of bevat code waarmee apps kunnen worden gedownload en geïnstalleerd, of
- Ten minste vijf procent van de apps die door de code worden gedownload zijn PHA's met een minimum drempel van 500 waargenomen app-downloads (25 waargenomen PHA-downloads).

Grote browsers en apps voor het delen van bestanden worden niet beschouwd als schadelijke downloaders op voorwaarde dat het volgende van toepassing is:

- Ze genereren geen downloads zonder interactie van de gebruiker, en
- Alle PHA-downloads worden gestart door gebruikers die hiervoor toestemming hebben gegeven.

## Niet-Android-dreiging

Code die niet-Android-dreigingen bevat.

Deze apps kunnen geen schade toebrengen aan de Android-gebruiker of het Android-apparaat, maar bevatten componenten die mogelijk schadelijk zijn voor andere platforms.

## Phishing

Code die doet alsof deze afkomstig is van een betrouwbare bron, verzoekt om de verificatie- of factureringsgegevens van een gebruiker en deze gegevens doorstuurt naar een derde. Deze categorie is ook van toepassing op code die de overdracht van inloggegevens van gebruikers onderschept tijdens de overdracht.

Veelvoorkomende doelen van phishing zijn onder meer bankgegevens, creditcardnummers en inloggegevens van online accounts voor sociale netwerken en games.

## Misbruik van hogere rechten

Code die de integriteit van het systeem in gevaar brengt door de sandbox van de app te doorbreken, rechten op een hoger niveau te verkrijgen of toegang tot belangrijke beveiligingsgerelateerde functies te wijzigen of uit te schakelen.

Voorbeelden hiervan zijn:

- een app die het rechtenmodel van Android schendt of inloggegevens (zoals OAuth-tokens) steelt uit andere apps,
- apps die functies misbruiken om te voorkomen dat ze worden verwijderd of gestopt,
- een app die SELinux uitschakelt.

Apps die zich rechten toe-eigenen en apparaten rooten zonder toestemming van de gebruiker, worden geclassificeerd als root-apps.

## Gijzelsoftware

Code die de gedeeltelijke of uitgebreide controle van een apparaat of gegevens op een apparaat overneemt en vereist dat de gebruiker een betaling uitvoert of een actie onderneemt om de controle te herstellen.

Sommige gijzelsoftware versleutelt gegevens op het apparaat en vraagt om een betaling om gegevens te ontsleutelen en/of gebruik te kunnen maken van de beheerdersfuncties, zodat deze niet kunnen worden verwijderd door een normale gebruiker. Voorbeelden hiervan zijn:

- een gebruiker de toegang tot zijn of haar apparaat ontzeggen en vragen om geld om de controle van de gebruiker te herstellen,
- gegevens op het apparaat versleutelen en vragen om een betaling, ogenschijnlijk om de gegevens te ontsleutelen,
- gebruikmaken van de beheerdersfuncties voor het apparaatbeleid en verwijdering door de gebruiker blokkeren.

Code die wordt verstrekt bij het apparaat waarvan het primaire doel uitbesteed apparaatbeheer is, kan worden uitgesloten van de categorie 'gijzelsoftware', mits deze voldoet aan de vereisten voor beveiligde vergrendeling en beheer en beschikt over toereikende kennisgevingen en toestemmingsvereisten voor gebruikers.

## Rooten

Code waarmee het apparaat wordt geroot.

Er is een verschil tussen niet-schadelijke en schadelijke root-code. Niet-schadelijke root-apps laten de gebruiker bijvoorbeeld van tevoren weten dat ze het apparaat gaan rooten en voeren geen andere mogelijk schadelijke acties uit die van toepassing zijn op andere PHA-categorieën.

Schadelijke root-apps laten de gebruiker niet weten dat ze het apparaat gaan rooten of stellen de gebruiker van tevoren op de hoogte van het rooten maar voeren ook andere acties uit die van toepassing zijn op andere PHA-categorieën.

### Spam

Code die ongevraagde berichten stuurt naar de contacten van de gebruiker of het apparaat gebruikt als relayservice voor spamberichten.

### Spyware

Code die persoonsgegevens verstuurt vanaf het apparaat zonder toereikende kennisgeving of toestemming.

De overdracht van de volgende informatie zonder kennisgeving of op een manier die de gebruiker niet verwacht, is bijvoorbeeld voldoende om als spyware te worden beschouwd:

- Contactenlijst
- Foto's of andere bestanden die op een SD-kaart staan of die geen eigendom zijn van de app
- Content uit gebruikersmail
- Gesprekslijst
- Sms-lijst
- Internetgeschiedenis of browserbookmarks van de standaardbrowser
- Informatie afkomstig uit de /data/-directories van andere apps.

Gedrag dat kan worden beschouwd als het bespioneren van de gebruiker, kan ook worden gemarkeerd als spyware. Bijvoorbeeld audio opnemen of gesprekken vastleggen die op de telefoon binnenkomen of app-gegevens stelen.

### Trojaans paard

Code die goedaardig lijkt te zijn, zoals een game die zegt alleen een game te zijn, maar toch ongewenste acties uitvoert tegen de gebruiker.

Deze indeling wordt meestal gebruikt in combinatie met andere PHA-categorieën. Een Trojaans paard beschikt over een onschadelijke component en een verborgen schadelijke component. Een voorbeeld is een game die op de achtergrond en zonder medeweten van de gebruiker premium sms-berichten verstuurt vanaf het apparaat van de gebruiker.

### Opmerkingen over ongebruikelijke apps

Nieuwe en zeldzame apps kunnen worden ingedeeld als 'ongebruikelijk' als Google Play Protect niet voldoende informatie heeft om ze als beveiligd in te delen. Dit houdt niet in dat de app noodzakelijkerwijs schadelijk is, maar zonder nadere beoordeling kan deze ook niet worden ingedeeld als beveiligd.

### Opmerkingen over de categorie 'backdoor'

De malwarecategorie 'backdoor' is gebaseerd op de manier waarop de code actief is. Code wordt geclassificeerd als een backdoor als deze gedrag mogelijk maakt waardoor de code in een van de andere malwarecategorieën zou worden ingedeeld als deze automatisch wordt uitgevoerd. Als een app bijvoorbeeld toestaat dat code dynamisch wordt geladen en de dynamisch geladen code sms-berichten extraheert, wordt deze ingedeeld als backdoor-malware.

Als een app echter toestaat dat code willekeurig wordt uitgevoerd en we geen reden hebben om aan te nemen dat de uitvoering van deze code is toegevoegd om schadelijk gedrag uit te voeren, wordt de app behandeld als een app met een kwetsbaarheid en niet als backdoor-malware. De ontwikkelaar wordt dan gevraagd een patch te ontwikkelen.

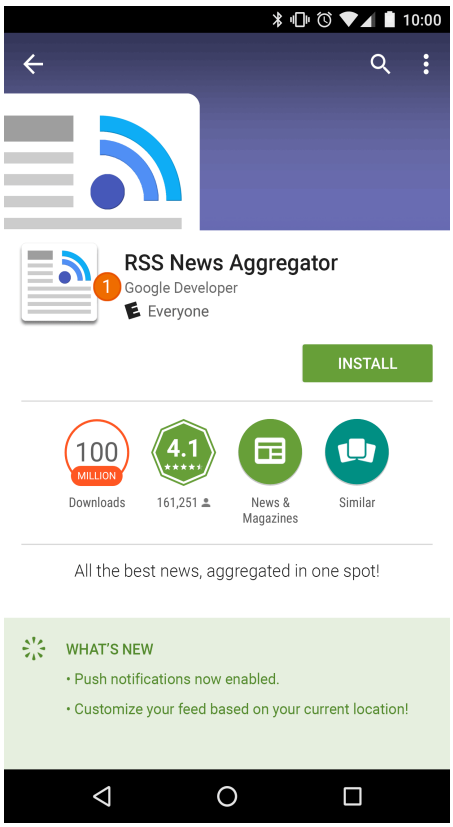
---

## Nabootsing van identiteit

We staan geen apps toe die gebruikers misleiden door zich voor te doen als iemand anders (bijvoorbeeld een ander(e) ontwikkelaar, bedrijf, entiteit) of een andere app. Wek niet de indruk dat uw app is gerelateerd aan of geautoriseerd door iemand anders als dat niet zo is.  Zorg ervoor dat u geen app-iconen, beschrijvingen, titels of in-app-elementen gebruikt die gebruikers kunnen misleiden over de relatie van uw app met iemand anders of een andere app.

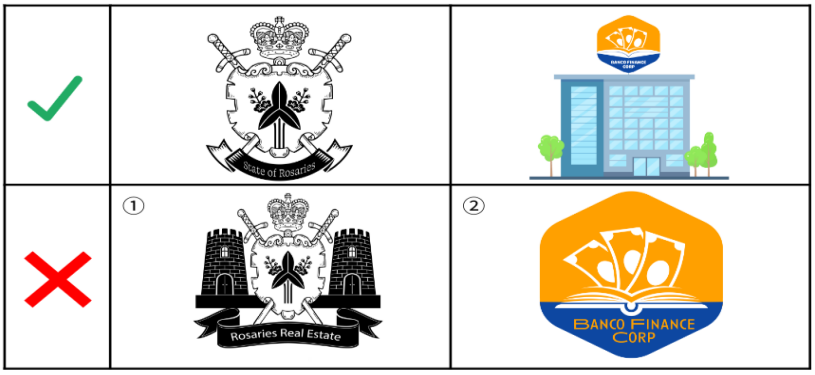
We hebben normen opgesteld die content definiëren en verbieden die schadelijk of ongepast is voor onze gebruikers om ervoor te zorgen dat Google Play een veilig en respectvol platform blijft.

- Ontwikkelaars die ten onrechte een relatie met een ander bedrijf, andere ontwikkelaar, andere entiteit of andere organisatie impliceren.




① De naam van de ontwikkelaar die voor deze app wordt vermeld, suggereert een officiële relatie met Google, ook al bestaat een dergelijke relatie niet.

- Apps waarvan de iconen en titel ten onrechte een relatie impliceren met een ander bedrijf, andere ontwikkelaar, andere entiteit of andere organisatie.




① De app gebruikt een nationaal symbool en misleidt gebruikers door hen de indruk te geven dat de app verband houdt met de overheid.
② De app kopieert het logo van een bedrijfsentiteit om ten onrechte de suggestie te wekken dat het een officiële app van het bedrijf is.

- De titel en iconen van een app lijken zo veel op die van bestaande producten of services dat gebruikers kunnen worden misleid.



① De app gebruikt het logo van een populaire cryptocurrencywebsite in zijn app-icoon om de suggestie te wekken dat het de officiële website is.
② De app kopieert het personage en de titel van een bekend tv-programma in zijn app-icoon, waardoor gebruikers ten onrechte denken dat de app verband houdt met een tv-programma.

- Apps die ten onrechte beweren de officiële app van een gevestigde entiteit te zijn. Een titel als 'Justin Bieber Official' is niet toegestaan zonder de noodzakelijke toestemming of rechten.
- Apps die in strijd zijn met de merkrichtlijnen van Android .

## Ongewenste mobiele software

Bij Google geloven we dat als we ons richten op de gebruiker, de rest vanzelf volgt. In onze softwareprincipes en het beleid voor ongewenste software geven we algemene aanbevelingen voor software die een goede gebruikerservaring biedt. Dit beleid is gebaseerd op het Google-beleid voor ongewenste software door de principes voor het en de Google Play Store te beschrijven. Software die

deze principes schendt, kan schadelijk zijn voor de gebruikerservaring en wij zullen stappen ondernemen om gebruikers er tegen te beschermen.

Zoals vermeld in het beleid voor ongewenste software, hebben we vastgesteld dat de meeste ongewenste software een of meer van dezelfde basiskenmerken heeft:

- De software is misleidend, de waardepropositie wordt niet nagekomen.
- Er wordt geprobeerd gebruikers over te halen de software te installeren of de software wordt samen met een ander programma geïnstalleerd.
- De software stelt de gebruiker niet op de hoogte van alle hoofdfuncties en andere belangrijke functies.
- De software beïnvloedt het systeem van de gebruiker op onverwachte manieren.
- De software verzamelt of verstuurt persoonlijke gegevens zonder medeweten van de gebruiker.
- De software verzamelt of verstuurt persoonlijke gegevens zonder een veilige afhandeling (bijvoorbeeld overdracht via HTTPS).
- De software wordt als onderdeel van een pakket geleverd (samen met andere software) en de aanwezigheid van die software wordt niet bekendgemaakt.

Op mobiele apparaten is software code in de vorm van een app, binair bestand, frameworkaanpassing, enz. We ondernemen actie tegen code die deze principes schendt om software die schadelijk is voor het software-ecosysteem of die de gebruikerservaring verstoort te voorkomen.

Hieronder gebruiken we het beleid voor ongewenste software als basis om de toepasselijkheid ervan uit te breiden naar mobiele software. Net als bij dat beleid zullen we dit beleid voor mobiele ongewenste software blijven verfijnen om nieuwe vormen van misbruik aan te pakken.

**Transparant gedrag en duidelijke openbaarmakingen**

*Alle code moet beloften die aan de gebruiker zijn gedaan waarmaken. Apps moeten alle meegedeelde functionaliteit bieden. Apps mogen gebruikers niet in verwarring brengen.*

- Apps moeten duidelijk zijn over de functionaliteit en doelen.
- Leg de gebruiker expliciet en duidelijk uit welke systeemwijzigingen door de app worden aangebracht. Stel gebruikers in staat alle belangrijke installatieopties en wijzigingen te bekijken en goed te keuren.
- Software mag de status van het apparaat van de gebruiker niet verkeerd weergeven aan de gebruiker, bijvoorbeeld door te claimen dat het systeem zich in een kritieke beveiligingsstatus bevindt of is geïnfecteerd met virussen.
- Gebruik geen ongeldige activiteit die is bedoeld om meer advertentieverkeer en/of meer conversies te genereren.
- We staan geen apps toe die gebruikers misleiden door zich voor te doen als iemand anders (bijvoorbeeld een andere ontwikkelaar, bedrijf, entiteit) of een andere app. Wek niet de indruk dat uw app is gerelateerd aan of geautoriseerd door iemand anders.

Voorbeelden van schendingen:

- Advertentiefraude
- Social engineering

**Bescherm gebruikersgegevens**

*Wees duidelijk en transparant over de toegang, het gebruik, de verzameling en het delen van persoonlijke en gevoelige gebruikersgegevens. Het gebruik van gebruikersgegevens moet voldoen aan alle relevante beleidsregels voor gebruikersgegevens, indien van toepassing, en alle voorzorgsmaatregelen nemen om de gegevens te beschermen.*

- Bied gebruikers de mogelijkheid om akkoord te gaan met de verzameling van hun gegevens voordat u deze vanaf het apparaat verzamelt en verstuurt, inclusief gegevens over accounts van derden, e-

mail, telefoonnummer, geïnstalleerde apps, bestanden, locatie en andere persoonlijke en gevoelige gegevens waarvan de gebruiker niet verwacht dat deze worden verzameld.
- Persoonlijke en gevoelige gebruikersgegevens die worden verzameld, moeten beveiligd worden verwerkt en moeten worden verstuurd via moderne cryptografie (bijvoorbeeld via HTTPS).
- Software, inclusief mobiele apps, mag alleen persoonlijke en gevoelige gebruikersgegevens naar servers sturen voor zover dit verband houdt met de functionaliteit van de app.

Voorbeelden van schendingen:

- Gegevensverzameling (zie Spyware)
- Misbruik van beperkte rechten

Voorbeeld van beleid voor gebruikersgegevens:

**Schaad de mobiele functionaliteit niet**

*De gebruikerservaring moet eenvoudig en begrijpelijk zijn en gebaseerd op duidelijke keuzes die de gebruiker heeft gemaakt. De functionaliteit moet een duidelijke waardepropositie bevatten voor de gebruiker en de geadverteerde of gewenste gebruikerservaring niet verstoren.*

- Geef geen advertenties weer die op onverwachte manieren aan gebruikers worden weergegeven, waardoor bijvoorbeeld de bruikbaarheid van apparaatfuncties wordt belemmerd of verstoord, of die buiten de trigger-omgeving van de app worden weergeven zonder gemakkelijk te kunnen worden gesloten en voldoende toestemming en toeschrijving.
- Apps mogen andere apps of de bruikbaarheid van het apparaat niet verstoren.
- De verwijdering, indien van toepassing, moet duidelijk zijn.
- Mobiele software mag geen prompts van het besturingssysteem van het apparaat of andere apps nabootsen. Onderdruk geen meldingen van andere apps of van het besturingssysteem voor de gebruiker, met name meldingen die de gebruiker informeren over wijzigingen in het besturingssysteem.

Voorbeelden van schendingen:

- Storende advertenties
- Onbevoegd gebruik of nabootsing van systeemfuncties

---

### Schadelijke downloaders

Code die zelf geen ongewenste software is, maar andere ongewenste mobiele software downloadt.

Code kan een schadelijke downloader zijn als:

- er reden is om aan te nemen dat de code is gemaakt om ongewenste mobiele software te verspreiden en de code ongewenste mobiele software gedownload heeft of code bevat waarmee apps kunnen worden gedownload en geïnstalleerd, of
- minimaal 5% van de apps die door de code worden gedownload, ongewenste mobiele software is met een minimumdrempel van 500 waargenomen app-downloads (25 waargenomen downloads van ongewenste mobiele software).

Grote browsers en apps voor het delen van bestanden worden niet beschouwd als schadelijke downloaders zolang:

- ze geen downloads genereren zonder interactie van de gebruiker, en
- alle softwaredownloads worden gestart door gebruikers die hiervoor toestemming hebben gegeven.

---

## Advertentiefraude

Advertentiefraude is ten strengste verboden. Advertentie-interacties die worden gegenereerd om een advertentienetwerk te laten geloven dat verkeer afkomstig is van oprechte interesse van gebruikers, is advertentiefraude, een vorm van ongeldig verkeer. Advertentiefraude kan het gevolg zijn van ontwikkelaars die advertenties op verboden manieren implementeren, zoals verborgen advertenties weergeven, automatisch op advertenties klikken, informatie wijzigen of aanpassen of op een andere manier gebruikmaken van niet-menselijke acties (spiders, bots, enzovoort) of menselijke activiteiten die zijn bedoeld om ongeldig advertentieverkeer te produceren. Ongeldig verkeer en advertentiefraude zijn schadelijk voor adverteerders, ontwikkelaars en gebruikers en leiden tot langdurig verlies van vertrouwen in het ecosysteem van mobiele advertenties.

We hebben normen opgesteld die content definiëren en verbieden die schadelijk of ongepast is voor onze gebruikers om ervoor te zorgen dat Google Play een veilig en respectvol platform blijft.

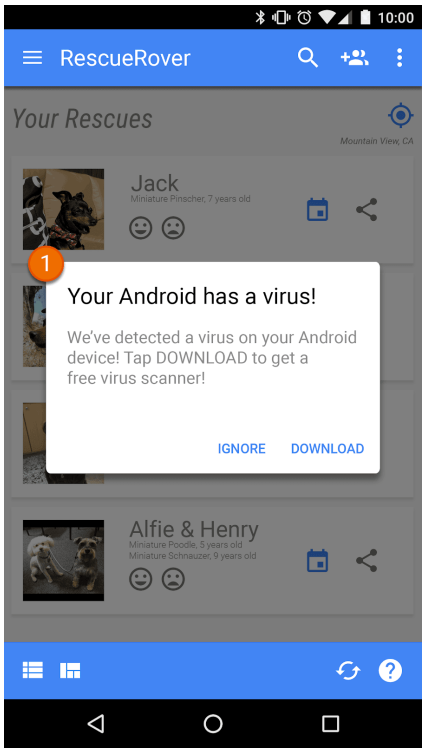
- Een app die advertenties weergeeft die niet zichtbaar zijn voor de gebruiker.
- Een app die automatisch klikken op advertenties genereert zonder de bedoeling van de gebruiker of die gelijkwaardig netwerkverkeer genereert om op frauduleuze wijze kliktegoeden te verstrekken.
- Een app die onjuiste klikken voor installatietoeschrijving verstuurt om betaald te worden voor installaties die niet afkomstig zijn van het netwerk van de afzender.
- Een app die advertenties weergeeft als de gebruiker zich niet in de app-interface bevindt.
- Valse verklaringen over de advertentievoorraad door een app, bijvoorbeeld een app die communiceert met advertentienetwerken dat deze wordt uitgevoerd op een iOS-apparaat terwijl deze daadwerkelijk wordt uitgevoerd op een Android-apparaat. Een app die een onjuiste voorstelling geeft van de pakketnaam waarmee inkomsten worden gegenereerd.

## Onbevoegd gebruik of nabootsing van systeemfuncties

We staan geen apps of advertenties toe die de systeemfunctionaliteit nabootsen of verstoren, zoals meldingen en waarschuwingen. Meldingen op systeemniveau mogen alleen worden gebruikt voor de integrale functies van een app, zoals de app van een luchtvaartmaatschappij die de gebruiker informeert over speciale aanbiedingen of een game die de gebruiker informeert over speciale aanbiedingen in de game.

We hebben normen opgesteld die content definiëren en verbieden die schadelijk of ongepast is voor onze gebruikers om ervoor te zorgen dat Google Play een veilig en respectvol platform blijft.

- Apps of advertenties die worden weergegeven door middel van een systeemmelding of -waarschuwing:




① De systeemmelding die in deze app wordt getoond, wordt gebruikt om een advertentie weer te geven.

Zie voor meer voorbeelden met advertenties het advertentiebeleid.

---

## Social engineering

We staan geen apps toe die zich voordoen als een andere app met de bedoeling gebruikers te misleiden om acties uit te voeren die de gebruikers wilden uitvoeren voor de oorspronkelijke vertrouwde app.

---

## Inkomsten genereren en advertenties

Google Play ondersteunt verschillende strategieën om inkomsten te genereren ten gunste van ontwikkelaars en gebruikers, waaronder betaalde distributie, in-app-producten, abonnementen en op advertenties gebaseerde modellen. Voor een optimale gebruikerservaring voor iedereen is de naleving van dit beleid van essentieel belang.

## Betalingen

1. Ontwikkelaars die kosten in rekening brengen voor app-downloads via Google Play, moeten het factureringssysteem van Google Play gebruiken als betaalmethode voor die transacties.
2. Via Play gedistribueerde apps die betaling vereisen of accepteren voor toegang tot in-app functies of services, waaronder app-functionaliteit, digitale content of artikelen (gezamenlijk 'in-app aankopen'), moeten het factureringssysteem van Google Play gebruiken voor die transacties, tenzij Artikel 3, 8 of 9 van toepassing is.

    Voorbeelden van app-functies of -services waarvoor het gebruik van het factureringssysteem van Google Play is vereist, zijn onder meer, maar niet uitsluitend, in-app aankopen van:

- items (zoals virtuele valuta's, extra levens, extra speeltijd, add-on-items, personages en avatars),
- abonnementsservices (zoals fitness, games, daten, onderwijs, muziek, video, service-upgrades en andere services voor contentabonnementen),
- app-functionaliteit of -content (zoals een app zonder advertenties of nieuwe functies die niet beschikbaar zijn in de kosteloze versie), en
- cloudsoftware en -services (zoals services voor gegevensopslag, software voor bedrijfsproductiviteit en software voor financieel beheer).

3. Het factureringssysteem van Google Play mag niet worden gebruikt in de volgende gevallen:
   a. De betaling vindt voornamelijk plaats:
      - voor de aankoop of verhuur van fysieke goederen (zoals boodschappen, kleding, huishoudelijke artikelen, elektronica),
      - voor de aankoop van fysieke services (zoals vervoersservices, schoonmaakservices, vluchten, sportschoollidmaatschappen, bezorging van eten, kaartjes voor live evenementen), of
      - een overschrijving met betrekking tot een creditcardafschrift of energierekening (zoals kabel- en telefoonservices),
   b. betalingen omvatten peer-to-peer-betalingen, online veilingen en belastingvrije donaties,
   c. de betaling is voor content of services die online kansspelen mogelijk maken, zoals beschreven in het gedeelte Apps voor kansspelen van het Beleid voor kansspelen, spellen en wedstrijden waarbij wordt gespeeld om echt geld,
   d. de betaling betreft een productcategorie die op grond van het Contentbeleid van het Betalingscentrum van Google als onacceptabel wordt beschouwd.

   Opmerking: In sommige markten bieden we Google Pay aan voor apps die fysieke goederen en/of services verkopen. Ga voor meer informatie naar onze Google Pay-ontwikkelaarspagina .

4. Behalve in de situaties die worden beschreven in Artikel 3, Artikel 8 en Artikel 9, mogen apps gebruikers niet naar een andere betaalmethode leiden dan het factureringssysteem van Google Play. Dit verbod omvat, maar is niet beperkt tot, gebruikers naar andere betaalmethoden leiden via:
   - een app-vermelding in Google Play,
   - in-app promoties met betrekking tot aanschafbare content,
   - in-app webweergaven, knoppen, links, berichten, advertenties of andere call-to-actions, en
   - gebruikersinterfacestromen in de app, waaronder het maken van of registreren voor een account, die gebruikers als onderdeel van die stromen van een app naar een andere betaalmethode dan het factureringssysteem van Google Play leiden.
5. Virtuele in-app valuta's mogen alleen worden gebruikt in de app of gametitel waarin ze zijn gekocht.
6. Ontwikkelaars moeten gebruikers duidelijk en nauwkeurig informeren over de voorwaarden en prijzen van hun app of in-app-functies of abonnementen die te koop worden aangeboden. In-app-prijzen moeten overeenkomen met de prijzen die worden weergegeven in de factureringsinterface van Play voor gebruikers. Als uw productbeschrijving op Google Play verwijst naar in-app-functies waarvoor specifieke of aanvullende kosten gelden, moet uw app-vermelding gebruikers duidelijk laten weten dat een betaling is vereist voor toegang tot die functies.
7. Apps en games die mechanismen aanbieden om willekeurige virtuele items te krijgen bij een aankoop (inclusief maar niet beperkt tot 'loot boxes'), moeten zowel vóór als tijdig en in de buurt van de aankoop duidelijk vermelden hoe groot de kans is dat de gebruiker die items krijgt.
8. Tenzij de voorwaarden van Artikel 3 van toepassing zijn, kunnen ontwikkelaars van via Play gedistribueerde apps die betaling vereisen of accepteren van gebruikers in deze landen/regio's voor toegang tot in-app aankopen, gebruikers voor die transacties ook een alternatief factureringssysteem aanbieden binnen de app naast het factureringssysteem van Google Play. Ze moeten daarvoor het declaratieformulier voor facturering voor het betreffende programma invullen

en akkoord gaan met de aanvullende voorwaarden en programmavereisten die daarin worden vermeld.

9. Ontwikkelaars van via Play gedistribueerde apps mogen gebruikers in de Europese Economische Ruimte (EER) omleiden naar een locatie buiten de app, onder meer om aanbiedingen voor digitale in-app functies en services te promoten. Ontwikkelaars die gebruikers in de EER omleiden naar een locatie buiten de app, moeten het declaratieformulier voor het programma invullen. Ook moeten ze akkoord gaan met de aanvullende voorwaarden en programmavereisten die daarin worden vermeld.

**Opmerking:** Ga naar ons Helpcentrum om tijdlijnen en veelgestelde vragen over dit beleid te bekijken.

---

## Advertenties

Voor een functionaliteit van hoge kwaliteit houden we rekening met de content, doelgroep, gebruikerservaring, gedragspatronen, beveiliging en privacy van uw app. We beschouwen advertenties en bijbehorende aanbiedingen als onderdeel van uw app, en deze moeten voldoen aan alle andere Google Play-beleidsregels. We hebben ook aanvullende vereisten voor advertenties als u inkomsten genereert met een app die is gericht op kinderen op Google Play.

U vindt hier meer informatie over ons Beleid voor app-promoties en winkelvermeldingen, waaronder hoe we omgaan met misleidende promoties.

### Content van de advertentie

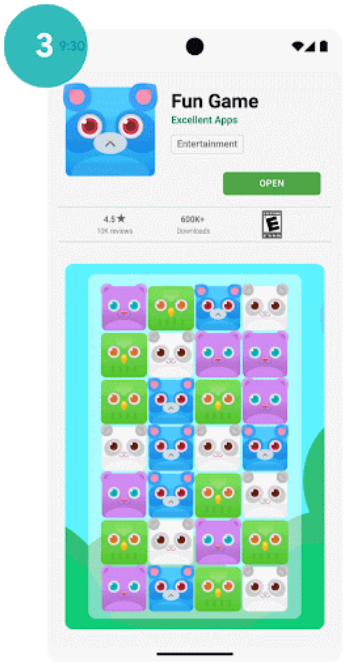
De advertenties en bijbehorende aanbiedingen maken deel uit van uw app en moeten voldoen aan ons Beleid voor beperkte content. Er zijn aanvullende vereisten van toepassing als uw app een kansspel-app is.

## Ongepaste advertenties

Advertenties en de bijbehorende aanbiedingen (de app promoot bijvoorbeeld het downloaden van een andere app) die worden weergegeven in uw app moeten geschikt zijn voor de contentclassificatie van uw app, zelfs als de content op zich voldoet aan ons beleid.

We hebben normen opgesteld die content definiëren en verbieden die schadelijk of ongepast is voor onze gebruikers om ervoor te zorgen dat Google Play een veilig en respectvol platform blijft.

- Advertenties die niet aansluiten op de contentclassificatie van de app


① Deze advertentie (Tieners) is ongepast voor de contentclassificatie van de app (Iedereen)
② Deze advertentie (Volwassenen) is ongepast voor de contentclassificatie van de app (Tieners)
③ De aanbieding van de advertentie (waarin het downloaden van een app voor volwassenen wordt gepromoot) is ongepast voor de contentclassificatie van de game-app waarin de advertentie werd weergegeven (Iedereen).

#### Vereisten voor advertenties voor gezinnen

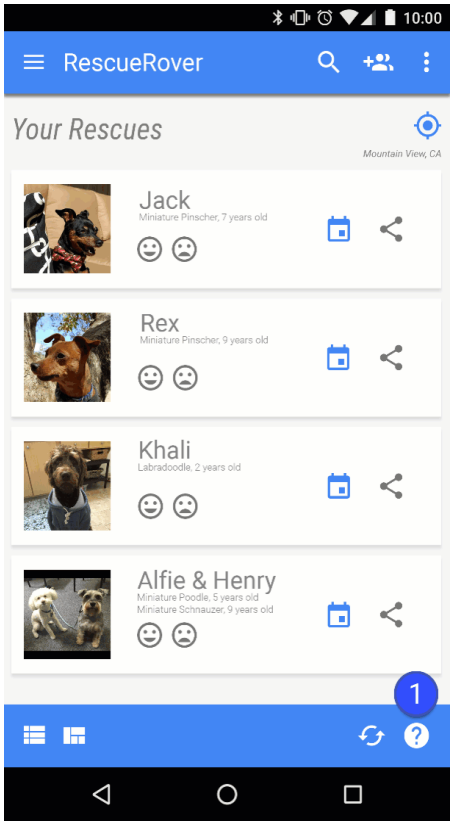
Als u inkomsten genereert met een app die kinderen target op Google Play, is het belangrijk dat uw app voldoet aan de vereisten van het Beleid voor advertenties voor gezinnen en inkomsten genereren.

## Misleidende advertenties

Advertenties mogen de gebruikersinterface van een app-functie, zoals meldings- of waarschuwingselementen van een besturingssysteem, niet simuleren of nabootsen. Het moet duidelijk zijn voor de gebruiker welke app een advertentie weergeeft.

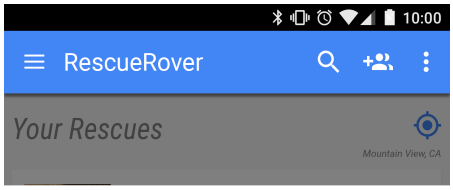
We hebben normen opgesteld die content definiëren en verbieden die schadelijk of ongepast is voor onze gebruikers om ervoor te zorgen dat Google Play een veilig en respectvol platform blijft.

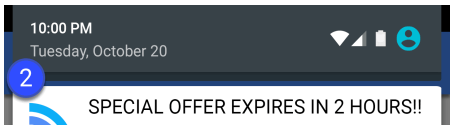
- Advertenties die de UI van een app nabootsen:




① Het vraagteken in deze app is een advertentie die de gebruiker omleidt naar een externe landingspagina.

- Advertenties die een systeemmelding nabootsen:






① ② De voorbeelden hierboven geven advertenties weer die verschillende systeemmeldingen nabootsen.

① Het voorbeeld hierboven toont een functiegedeelte dat andere functies nabootst, maar de gebruiker alleen omleidt naar een advertentie of advertenties.

## Storende advertenties

Storende advertenties zijn advertenties die op onverwachte manieren aan gebruikers worden getoond, die kunnen leiden tot onbedoelde klikken of die de bruikbaarheid van apparaatfuncties belemmeren of verstoren.

Uw app mag een gebruiker niet dwingen om op een advertentie te klikken of persoonlijke informatie voor advertentiedoeleinden te verstrekken voordat die een app volledig kan gebruiken. Advertenties mogen alleen worden getoond in de app die ze weergeeft en mogen geen verstoring vormen voor andere apps, advertenties of de werking van het apparaat, waaronder systeem- of apparaatknoppen en -poorten. Dit geldt onder andere voor overlays, bijbehorende functies en advertentieblokken met een widget. Als uw app advertenties of andere advertenties toont die het normale gebruik verstoren, moeten ze makkelijk te sluiten zijn zonder dat dit tot problemen leidt.

We hebben normen opgesteld die content definiëren en verbieden die schadelijk of ongepast is voor onze gebruikers om ervoor te zorgen dat Google Play een veilig en respectvol platform blijft.

- Advertenties die het hele scherm vullen of die het normale gebruik verstoren en geen duidelijke mogelijkheid geven om de advertentie te sluiten:



① Deze advertentie heeft geen sluitknop.

- Advertenties die de gebruiker dwingen door te klikken via een valse sluitknop of door advertenties plotseling te laten verschijnen in gedeelten van de app waar de gebruiker meestal op een andere functie tikt:

① Deze advertentie heeft een valse sluitknop.

② Deze advertentie verschijnt plotseling in een gedeelte waar de gebruiker gewend is te tikken voor in-app functies.

- Advertenties die worden weergegeven buiten de app waarin ze worden getoond:

① De gebruiker gaat naar het startscherm vanuit deze app, en er wordt plotseling een advertentie op het startscherm getoond.

- Advertenties die worden geactiveerd door de startknop of andere functies die uitdrukkelijk zijn ontworpen om de app te verlaten:

① De gebruiker probeert de app te verlaten en naar het startscherm te gaan, maar de verwachte gang van zaken wordt verstoord door een advertentie.

**Betere advertentiebelevingen**

Ontwikkelaars moeten voldoen aan de volgende advertentierichtlijnen om een hoogwaardige beleving te waarborgen voor gebruikers wanneer zij Google Play-apps gebruiken. Uw advertenties mogen op de volgende onverwachte manieren niet worden getoond aan gebruikers:

- Interstitial-advertenties op volledig scherm in alle indelingen (video, gif, statisch, enzovoort) die onverwacht worden getoond, meestal wanneer de gebruiker ervoor heeft gekozen iets anders te doen, zijn niet toegestaan.
  - Advertenties die verschijnen tijdens de gameplay aan het begin van een level of aan het begin van een contentsegment zijn niet toegestaan.
  - Interstitial-advertenties in beeldvullende video die worden weergegeven voor het laadscherm van een app (startscherm) zijn niet toegestaan.
- Interstitial-advertenties op volledig scherm in alle indelingen die niet na vijftien (15) seconden kunnen worden gesloten, zijn niet toegestaan. Interstitial-advertenties op volledig scherm waarvoor toestemming is gegeven of interstitial-advertenties op volledig scherm die gebruikers niet onderbreken tijdens hun acties (bijvoorbeeld na het scorescherm in een game-app) mogen langer dan vijftien (15) seconden worden weergegeven.

Dit beleid is niet van toepassing op advertenties met beloning waarvoor gebruikers expliciet toestemming verlenen (bijvoorbeeld advertenties die ontwikkelaars expliciet aanbieden aan gebruikers om te kijken in ruil voor het ontgrendelen van een specifieke functie in de game of een contentonderdeel). Dit beleid is ook niet van toepassing op het genereren van inkomsten en advertenties die het normale gebruik van de app of de normale gameplay niet onderbreken (bijvoorbeeld videocontent met geïntegreerde advertenties en banneradvertenties die niet op volledig scherm worden weergegeven).

Deze richtlijnen zijn gebaseerd op de richtlijnen Better Ads Standards (normen voor betere advertenties). Bezoek de website van de Coalition for Better Ads voor meer informatie over Better Ads Standards (normen voor betere advertenties).

We hebben normen opgesteld die content definiëren en verbieden die schadelijk of ongepast is voor onze gebruikers om ervoor te zorgen dat Google Play een veilig en respectvol platform blijft.

- Onverwachte advertenties die worden weergegeven tijdens de gameplay of aan het begin van een contentsegment (bijvoorbeeld nadat de gebruiker op een knop heeft geklikt en voordat de met de knop beoogde actie wordt geactiveerd). Deze advertenties worden door gebruikers niet verwacht, aangezien ze verwachten met een game te beginnen of dat content wordt geactiveerd.

① Onverwachte statische advertentie die wordt weergegeven tijdens de gameplay aan het begin van een level.

② Onverwachte videoadvertentie die wordt weergegeven aan het begin van een contentsegment.

- Een advertentie op volledig scherm die wordt weergegeven tijdens de gameplay en niet na vijftien (15) seconden kan worden gesloten.

① Een interstitial-advertentie die wordt weergegeven tijdens de gameplay en die gebruikers niet binnen 15 seconden de optie biedt om de advertentie over te slaan.

## Gemaakt voor advertenties

We staan geen apps toe die herhaaldelijk interstitial-advertenties weergegeven en zo gebruikers onderbreken bij de interactie met de app en de uitvoering van taken in de app verstoren.

We hebben normen opgesteld die content definiëren en verbieden die schadelijk of ongepast is voor onze gebruikers om ervoor te zorgen dat Google Play een veilig en respectvol platform blijft.

- Apps waarin opeenvolgende interstitial-advertenties worden geplaatst na een actie van de gebruiker (waaronder, maar niet beperkt tot klikken, swipen, enzovoort).

① De eerste pagina in de app beschikt over meerdere knoppen voor interactie. Als de gebruiker op **App starten** klikt om de app te gebruiken, wordt een interstitial-advertentie weergegeven.Nadat de advertentie is gesloten, keert de gebruiker terug naar de app en klikt op **Service** om de service te gebruiken, maar vervolgens wordt weer een interstitial-advertentie weergegeven.

② Op de eerste pagina wordt de gebruiker geleid naar de knop **Afspelen**, aangezien dit de enige knop is die beschikbaar is om de app te gebruiken. Als de gebruiker erop klikt, wordt een interstitial-advertentie weergegeven. Nadat de advertentie is gesloten, klikt de gebruiker op **Starten**, aangezien dit de enige knop is waarmee interactie mogelijk is, waarna weer een interstitial-advertentie wordt weergegeven.

## Inkomsten genereren met een vergrendelingsscherm

Tenzij de app exclusief is bedoeld als vergrendelingsscherm, mogen apps geen advertenties of functies introduceren waarmee inkomsten worden gegenereerd via het vergrendelde scherm van een apparaat.

### Advertentiefraude

Advertentiefraude is ten strengste verboden. Meer informatie vindt u in ons Beleid tegen advertentiefraude.

## Gebruik van locatiegegevens voor advertenties

Apps die het gebruik van op rechten gebaseerde locatiegegevens van het apparaat uitbreiden voor de weergave van advertenties, vallen onder het beleid voor persoonlijke en gevoelige gegevens en moeten ook voldoen aan de volgende vereisten:

- Het gebruik of de verzameling van op rechten gebaseerde locatiegegevens van het apparaat voor advertentiedoeleinden moet duidelijk zijn voor de gebruiker en vastgelegd in het verplichte privacybeleid van de app, met inbegrip van links naar de privacybeleidsregels van advertentienetwerken die van toepassing zijn op het gebruik van locatiegegevens.
- In overeenstemming met de vereisten voor locatierechten mogen locatierechten alleen worden opgevraagd voor de uitvoering van de betreffende functies of services in uw app en mogen niet vragen om locatierechten van het apparaat uitsluitend voor het gebruik van advertenties.

## Gebruik van de Android-advertentie-ID

In Google Play-services versie 4.0 zijn nieuwe API's geïntroduceerd, evenals een ID die is bedoeld voor gebruik door advertentie- en analyseleveranciers. U vindt de gebruiksvoorwaarden voor deze ID hieronder.

- **Gebruik**. De Android-advertentie-ID (AAID) mag alleen worden gebruikt voor advertentie- en gebruikersanalyse. De status van de instelling 'Afmelden voor op interesses gebaseerd adverteren' of 'Afmelden voor personalisatie van advertenties' moet worden geverifieerd bij elke toegang tot de ID.
- **Koppeling aan persoonlijk identificeerbare informatie of andere ID's**.
  - Advertentiegebruik: De advertentie-ID mag niet voor advertentiedoeleinden worden gekoppeld aan permanente apparaat-ID's (zoals SSAID, MAC-adres, IMEI, enzovoort). De advertentie-ID mag alleen na uitdrukkelijke toestemming van de gebruiker worden gekoppeld aan persoonlijk identificeerbare informatie.
  - Analysegebruik: De advertentie-ID mag niet voor analysedoeleinden worden gekoppeld aan persoonlijk identificeerbare informatie of permanente apparaat-ID's (zoals SSAID, MAC-adres, IMEI, enzovoort). Lees het Beleid voor gebruikersgegevens voor meer richtlijnen voor permanente apparaat-ID's.
- **Selecties van gebruikers respecteren**.
  - Bij opnieuw instellen mag een nieuwe advertentie-ID niet zonder uitdrukkelijke toestemming van de gebruiker worden gekoppeld aan een eerdere advertentie-ID of gegevens die zijn afgeleid van een eerdere advertentie-ID.
  - U moet de instelling 'Afmelden voor op interesses gebaseerd adverteren' of 'Afmelden voor personalisatie van advertenties' van een gebruiker respecteren. Als een gebruiker deze instelling heeft aangezet, mag u de advertentie-ID niet gebruiken om gebruikersprofielen voor advertentiedoeleinden te maken of om gepersonaliseerde advertenties op gebruikers te targeten. Toegestane activiteiten omvatten contextueel adverteren, frequentielimieten, het bijhouden van conversies, rapportage en beveiliging en fraudedetectie.
  - Op nieuwere apparaten wordt de Android-advertentie-ID verwijderd als een gebruiker deze verwijdert. Bij elke poging om de ID op te vragen, wordt een tekenreeks met nullen ontvangen. Een apparaat zonder advertentie-ID mag niet worden gekoppeld aan gegevens die zijn gekoppeld aan of afgeleid van een eerdere advertentie-ID.
- **Transparantie voor gebruikers**. Het feit dat de advertentie-ID wordt verzameld en gebruikt en dat u deze voorwaarden naleeft, moet openbaar worden gemaakt aan gebruikers in een privacymelding die voldoet aan de wettelijke vereisten. Raadpleeg ons beleid voor gebruikersgegevens voor meer informatie over onze privacynormen.
- **Gebruiksvoorwaarden naleven**. De advertentie-ID mag alleen worden gebruikt in overeenstemming met het Programmabeleid voor ontwikkelaars van Google Play. Dit geldt ook voor derden waarmee u deze advertentie-ID deelt tijdens de uitvoering van uw zakelijke werkzaamheden. Alle apps die worden geüpload naar of gepubliceerd op Google Play moeten de advertentie-ID (indien beschikbaar op een apparaat) in plaats van andere apparaat-ID's gebruiken voor advertentiedoeleinden.

Raadpleeg ons Beleid voor gebruikersgegevens voor meer informatie.

# Abonnementen

Als ontwikkelaar mag u gebruikers niet misleiden over de abonnementsservices of -content die u aanbiedt binnen uw app. Het is uiterst belangrijk dat u in promoties in de app of op startschermen duidelijk communiceert over wat u aanbiedt. We staan geen apps toe die gebruikers onderwerpen aan misleidende of manipulatieve aankoopprocessen (waaronder in-app-aankopen of abonnementen).

U moet transparant zijn over uw aanbieding. Dit houdt onder meer in dat u duidelijk moet zijn over de voorwaarden van de aanbieding, de kosten van het abonnement, hoe vaak u factureert en of gebruikers een abonnement nodig hebben om de app te kunnen gebruiken. Gebruikers moeten deze informatie zonder extra handelingen kunnen bekijken.

Abonnementen moeten blijvende of terugkerende waarde bieden aan gebruikers gedurende de looptijd van het abonnement en mogen niet worden gebruikt om items aan te bieden die in feite eenmalige voordelen zijn (zoals SKU's die eenmalig in-app-tegoeden/-valuta's bieden of gameboosters die één keer gebruikt kunnen worden). Uw abonnement mag beloningen of promotiebonussen bieden, maar deze moeten een aanvulling zijn op de blijvende of terugkerende waarde die gedurende de looptijd van het abonnement wordt geboden. Voor producten die geen blijvende of terugkerende waarde bieden, moet u een in-app-product in plaats van een abonnementsproduct gebruiken.

U mag eenmalige voordelen voor gebruikers niet vermommen of verkeerd voorstellen als abonnementen. Dit omvat de aanpassing van een abonnement om er een eenmalige aanbieding van te maken (bijvoorbeeld door de terugkerende waarde te annuleren, te beëindigen of te minimaliseren) nadat de gebruiker het abonnement heeft aangeschaft.

We hebben normen opgesteld die content definiëren en verbieden die schadelijk of ongepast is voor onze gebruikers om ervoor te zorgen dat Google Play een veilig en respectvol platform blijft.

- Maandabonnementen waarbij de gebruiker niet wordt geïnformeerd over de automatische maandelijkse verlenging en de kosten die daaruit voortkomen.
- Jaarabonnementen waarbij de meest zichtbare prijs de kosten per maand weergeeft.
- Abonnementsprijzen en -voorwaarden die niet volledig zijn gelokaliseerd.
- In-app-promoties die niet duidelijk aangeven dat een gebruiker toegang heeft tot de content zonder een abonnement (indien beschikbaar).
- SKU-namen die niet duidelijk maken wat de aard van het abonnement is, zoals 'Kosteloze proefperiode' of 'Probeer het Premium-lidmaatschap 3 dagen zonder kosten' voor een abonnement waarvan de verlenging telkens automatisch in rekening wordt gebracht.
- Meerdere vensters in het aankoopproces die ertoe leiden dat gebruikers onbedoeld op de knop Abonneren klikken.
- Abonnementen die geen blijvende of terugkerende waarde bieden. Ze bieden bijvoorbeeld 1000 edelstenen voor de eerste maand en daarna wordt het voordeel beperkt tot 1 edelsteen in de daaropvolgende maanden van het abonnement.
- Vereisen dat een gebruiker zich aanmeldt voor een abonnement met automatische verlenging om een eenmalig voordeel te leveren en het abonnement van een gebruiker na de aankoop opzeggen zonder dat de gebruiker daarvoor een verzoek heeft ingediend.

**Voorbeeld 1:**

① De knop Sluiten is niet duidelijk zichtbaar en gebruikers begrijpen misschien niet dat ze toegang tot de functionaliteit hebben zonder het aangeboden abonnement te accepteren.

② De aanbieding geeft alleen de kosten per maand weer en gebruikers begrijpen mogelijk niet dat de kosten voor zes maanden in rekening worden gebracht op het moment dat ze zich abonneren.

③ De aanbieding geeft alleen de introductieprijs weer en gebruikers begrijpen mogelijk niet welk bedrag automatisch in rekening wordt gebracht na afloop van de introductieperiode.

④ De aanbieding moet zijn gelokaliseerd in dezelfde taal als de algemene voorwaarden zodat gebruikers de volledige aanbieding kunnen begrijpen.

**Voorbeeld 2:**

① Herhaalde klikken in hetzelfde knopgebied die ertoe leiden dat de gebruiker onbedoeld op de laatste knop Doorgaan klikt om zich te abonneren.

② Het bedrag dat na afloop van de proefperiode aan gebruikers in rekening wordt gebracht is moeilijk te lezen, waardoor gebruikers misschien denken dat er geen kosten aan het abonnement zijn verbonden.

## Kosteloze proefperioden en introductieaanbiedingen

**Voordat een gebruiker wordt aangemeld voor uw abonnement:** U moet een duidelijke en nauwkeurige beschrijving geven van de voorwaarden van uw aanbieding, waaronder de duur, de prijzen en een beschrijving van de toegankelijke content of services. Laat uw gebruikers weten hoe en wanneer een kosteloze proefperiode wordt omgezet in een betaald abonnement, hoeveel het betaalde abonnement kost. Vermeld ook dat ze het abonnement kunnen opzeggen als ze niet willen worden overgezet naar een betaald abonnement.

We hebben normen opgesteld die content definiëren en verbieden die schadelijk of ongepast is voor onze gebruikers om ervoor te zorgen dat Google Play een veilig en respectvol platform blijft.

- Aanbiedingen waarbij niet duidelijk wordt aangegeven hoelang de kosteloze proefperiode of de introductieprijs duurt.
- Aanbiedingen waarbij niet duidelijk wordt aangegeven dat de gebruiker automatisch wordt overgezet naar een betaald abonnement aan het einde van de aanbiedingsperiode.
- Aanbiedingen waarbij niet duidelijk wordt aangegeven dat een gebruiker toegang heeft tot content zonder een proefperiode (indien beschikbaar).
- Aanbiedingsprijzen en -voorwaarden die niet volledig zijn gelokaliseerd.

① De knop 'Sluiten' is niet duidelijk zichtbaar en gebruikers begrijpen mogelijk niet dat ze toegang tot de functionaliteit hebben zonder zich aan te melden voor een kosteloze proefperiode.

② De aanbieding benadrukt de kosteloze proefperiode en gebruikers begrijpen mogelijk niet dat aan het einde van de kosteloze proefperiode automatisch een bedrag in rekening wordt gebracht.

③ In de aanbieding staat geen proefperiode vermeld en gebruikers begrijpen mogelijk niet hoe lang de kosteloze toegang tot abonnementscontent duurt.

④ De aanbieding moet zijn gelokaliseerd in dezelfde taal als de algemene voorwaarden zodat gebruikers de volledige aanbieding kunnen begrijpen.

**Abonnementen beheren en opzeggen en terugbetalingen**

Als u abonnementen verkoopt in uw app(s) moet u ervoor zorgen dat uw app(s) duidelijk aangeeft/aangeven hoe een gebruiker het abonnement kan beheren of opzeggen. Uw app moet ook toegang bevatten tot een eenvoudig te gebruiken online manier om het abonnement op te zeggen. In de accountinstellingen van uw app (of op een soortgelijke pagina) kunt u aan deze vereiste voldoen door het volgende te vermelden:

- een link naar het abonnementscentrum van Google Play (voor apps die gebruik maken van het factureringssysteem van Google Play), en/of

- rechtstreekse toegang tot uw opzeggingsprocedure.

Als een gebruiker een abonnement opzegt dat via het factureringssysteem van Google Play is gekocht op Google Play, is het ons algemene beleid dat de gebruiker geen terugbetaling ontvangt voor de huidige factureringsperiode, maar tijdens de rest van de huidige factureringsperiode de abonnementscontent blijft ontvangen, ongeacht de datum van opzegging. De opzegging van de gebruiker gaat in nadat de huidige factureringsperiode is afgelopen.

U (als leverancier van de content of toegang) mag uw gebruikers rechtstreeks een flexibeler teruggavebeleid bieden. Het is uw verantwoordelijkheid om gebruikers te informeren over wijzigingen in uw abonnements-, opzeggings- en teruggavebeleid en ervoor te zorgen dat uw beleid voldoet aan de toepasselijke wetgeving.

---

## Zelfgecertificeerde advertentie-SDK's voor gezinnen

Als u advertenties weergeeft in uw app en de doelgroep uitsluitend uit kinderen bestaat zoals beschreven in het Gezinsbeleid , mag u alleen versies van advertentie-SDK's gebruiken met zelfgecertificeerde naleving van het beleid van Google Play, met inbegrip van de onderstaande vereisten voor zelfgecertificeerde advertentie-SDK's voor gezinnen.

Als de doelgroep van uw app uit zowel kinderen als oudere gebruikers bestaat, moet u zorgen dat advertenties die aan kinderen worden getoond uitsluitend afkomstig zijn van een versie van deze zelfgecertificeerde advertentie-SDK's (bijvoorbeeld door gebruik van een neutraal leeftijdsscherm).

Houd er rekening mee dat het uw verantwoordelijkheid is om te controleren of alle SDK-versies die u in uw app implementeert, waaronder versies van zelfgecertificeerde advertentie-SDK's, voldoen aan alle toepasselijke beleid en de lokale wet- en regelgeving. Google verstrekt geen verklaringen of garanties met betrekking tot de nauwkeurigheid van de gegevens die de advertentie-SDK's tijdens het zelfcertificeringsproces leveren.

Het gebruik van zelfgecertificeerde advertentie-SDK's voor gezinnen is alleen vereist als u advertentie-SDK's gebruikt om advertenties weer te geven aan kinderen. Hoewel u er bij het gebruik van advertentiecontent en gegevensverzameling nog steeds verantwoordelijk voor bent dat u het Beleid voor gebruikersgegevens en het Gezinsbeleid van Google Play naleeft, is het volgende toegestaan zonder de zelfcertificering van een advertentie-SDK bij Google Play:

- Zelf adverteren op eigen advertentieplekken, waarbij u SDK's gebruikt om crosspromotie van uw apps of andere eigen media en merchandising te beheren.
- Directe deals afsluiten met adverteerders, waarbij u SDK's gebruikt voor voorraadbeheer.

**Vereisten voor zelfgecertificeerde advertentie-SDK's voor gezinnen**

- Definieer wat aanstootgevende advertentiecontent en aanstootgevend gedrag inhoudt en verbied deze in de voorwaarden of het beleid van de advertentie-SDK. De definities moeten voldoen aan het Programmabeleid voor ontwikkelaars van Google Play.
- Ontwikkel een methode om uw advertentiemateriaal te classificeren voor specifieke leeftijdsgroepen. Gebruik minimaal de leeftijdsgroepen Iedereen en Volwassenen. De methode van classificatie moet overeenstemmen met de methode die Google gebruikt voor SDK's nadat het onderstaande interesseformulier ingevuld is.
- Maak het voor uitgevers mogelijk om, per verzoek of per app, een behandeling van content die bedoeld is voor kinderen aan te vragen voor het weergeven van advertenties. Deze behandeling moet voldoen aan de toepasselijke wet- en regelgeving, zoals de Amerikaanse Children's Online Privacy and Protection Act (COPPA) en de Algemene verordening gegevensbescherming (AVG) van de EU . Google Play vereist dat advertentie-SDK's gepersonaliseerde advertenties, op interesses gebaseerd adverteren en remarketing uitzetten als onderdeel van de behandeling van content die bedoeld is voor kinderen.
- Sta uitgevers toe advertentie-indelingen te selecteren die voldoen aan het Beleid voor advertenties voor gezinnen en inkomsten genereren van Google Play en aan de vereisten van het programma

Goedgekeurd door docenten .

- Als realtime bieden wordt gebruikt om advertenties weer te geven aan kinderen, zorg dan dat het advertentiemateriaal is beoordeeld en dat de privacyindicatoren aan de bieders bekend worden gemaakt.
- Geef Google voldoende informatie, zoals een test-app en de informatie die op het onderstaande interesseformulier is vermeld, om te kunnen verifiëren of de advertentie-SDK aan alle zelfcertificeringsvereisten voldoet. Reageer ook tijdig op elk vervolgverzoek om informatie, met bijvoorbeeld nieuwe versiereleases om te verifiëren of de advertentie-SDK aan alle zelfcertificeringsvereisten voldoet en een nieuwe test-app.
- Check door middel van zelfcertificering of alle nieuwe versiereleases voldoen aan het meest recente Programmabeleid voor ontwikkelaars van Google Play, waaronder de vereisten voor Gezinsbeleid.

*Opmerking: Zelfgecertificeerde advertentie-SDK's voor gezinnen moeten de weergave van advertenties ondersteunen die voldoet aan alle relevante wet- en regelgeving betreffende kinderen die mogelijk van toepassing is op hun uitgevers.*

Hier vindt u meer informatie over hoe u watermerken toevoegt aan advertentiemateriaal en een test-app levert.

Dit zijn bemiddelingsvereisten voor weergaveplatforms als deze advertenties weergeven aan kinderen:

- Gebruik alleen zelfgecertificeerde advertentie-SDK's voor gezinnen of gebruik andere waarborgen om ervoor te zorgen dat alle via bemiddeling weergegeven advertenties voldoen aan deze vereisten.
- Geef noodzakelijke informatie door aan bemiddelingsplatforms om de classificatie voor advertentiecontent en eventueel toepasselijke behandeling van content die bedoeld is voor kinderen aan te geven.

Ontwikkelaars kunnen hier een lijst van zelfgecertificeerde advertentie-SDK's voor gezinnen vinden en checken welke specifieke versies van die advertentie-SDK's zelfgecertificeerd zijn voor gebruik in gezinsapps.

Ontwikkelaars kunnen ook dit interesseformulier delen met advertentie-SDK's die zelfgecertificeerd willen worden.

---

# Winkelvermelding en promotie

De promotie en zichtbaarheid van uw app zijn van grote invloed op de kwaliteit van de winkel. Vermijd spamachtige winkelvermeldingen, promoties van lage kwaliteit en activiteiten om de zichtbaarheid van de app op Google Play kunstmatig te verhogen.

## App-promotie

We staan geen apps toe die direct of indirect betrokken zijn bij of profiteren van promotiepraktijken (zoals advertenties) die misleidend of schadelijk zijn voor gebruikers of het ecosysteem van ontwikkelaars. Promotiepraktijken zijn misleidend of schadelijk als het gedrag of de content in strijd is met ons Programmabeleid voor ontwikkelaars.

We hebben normen opgesteld die content definiëren en verbieden die schadelijk of ongepast is voor onze gebruikers om ervoor te zorgen dat Google Play een veilig en respectvol platform blijft.

- Het gebruik van misleidende advertenties op websites, in apps of in andere services, waaronder meldingen die lijken op systeemmeldingen en -waarschuwingen.
- Het gebruik van seksueel expliciete advertenties om gebruikers naar de Google Play-vermelding van uw app te leiden om de app te downloaden.
- Promotie- of installatietactieken waarbij gebruikers worden omgeleid naar Google Play of die apps downloaden zonder dat de gebruiker hier bewust voor kiest.

- Ongevraagde promotie via sms-services.
- Tekst of afbeelding in de app-titel, het icoon of de naam van de ontwikkelaar die de prestaties of positie in de winkel, de prijs of promotie-informatie aangeeft of die een relatie met bestaande Google Play-programma's suggereert.

Het is uw verantwoordelijkheid om ervoor te zorgen dat advertentienetwerken, partners of advertenties die zijn gekoppeld aan uw app, voldoen aan dit beleid.

---

## Metadata

Gebruikers zijn afhankelijk van beschrijvingen van uw app om inzicht te krijgen in de functionaliteit en het doel van de app. We staan geen apps toe met misleidende, onjuist opgemaakte, niet-beschrijvende, irrelevante, buitensporige of ongepaste metadata, inclusief maar niet beperkt tot de beschrijving van de app, de naam van de ontwikkelaar, de titel, het icoon, screenshots en promotieafbeeldingen. Ontwikkelaars moeten een duidelijke en goed geformuleerde beschrijving van hun app geven. We staan ook geen niet-herleidbare of anonieme gebruikerservaringen toe in de beschrijving van de app.

Uw app-titel, icoon en ontwikkelaarsnaam zijn met name nuttig voor gebruikers om uw app te vinden en meer informatie hierover te krijgen. Gebruik geen emoji's, emoticons of herhaalde speciale tekens in deze metadata-elementen. Vermijd tekst in HOOFDLETTERS tenzij dit deel uitmaakt van uw merknaam. Misleidende symbolen in app-iconen zijn niet toegestaan, zoals een meldingsstipje voor nieuwe berichten als er geen nieuwe berichten zijn en download-/installatiesymbolen als de app niets te maken heeft met het downloaden van content. Uw app-titel mag maximaal 30 tekens lang zijn. Gebruik geen tekst of afbeelding in de app-titel, het icoon of de naam van de ontwikkelaar die de prestaties of positie in de winkel, de prijs of promotie-informatie aangeeft of die een relatie met bestaande Google Play-programma's suggereert.

In aanvulling op de hier vermelde vereisten is het op grond van specifiek Beleid voor Google Play-ontwikkelaars mogelijk noodzakelijk om aanvullende metadata-informatie te verstrekken.

We hebben normen opgesteld die content definiëren en verbieden die schadelijk of ongepast is voor onze gebruikers om ervoor te zorgen dat Google Play een veilig en respectvol platform blijft.

① Niet-herleidbare of anonieme gebruikerservaringen
② Gegevensvergelijking van apps of merken
③ Blokken met woorden en verticale/horizontale lijsten met woorden

① Tekst in HOOFDLETTERS die niet deel is van de merknaam
② Herhaalde speciale tekens die niet relevant zijn voor de app
③ Gebruik van emoji's, emoticons (waaronder kaomoji's) en speciale tekens
④ Misleidend symbool
⑤ Misleidende tekst

- Afbeeldingen of tekst die de prestaties of positie in de winkel aangeven, zoals App van het jaar, nr. 1, Het beste van Play 20XX, Populair, iconen van awards, enzovoort

- Afbeeldingen of tekst die prijs- en promotiegegevens aangeven, zoals 10% korting, € 50 cashback, tijdelijk gratis beschikbaar, enzovoort

- Afbeeldingen of tekst die Google Play-programma's aangeven, zoals Keuze van de redactie, Nieuw, enzovoort

**Dit zijn enkele voorbeelden van ongepaste tekst, afbeeldingen of video's in uw vermelding:**

- Afbeeldingen of video's met seksueel suggestieve content. Vermijd suggestieve afbeeldingen met borsten, billen, genitaliën of andere geseksualiseerde lichaamsdelen of content, ongeacht of deze geïllustreerd of echt zijn.
- Het gebruik van grof, vulgair of ander taalgebruik dat ongepast is voor een algemeen publiek in de winkelvermelding van uw app.
- Extreem geweld dat prominent wordt afgebeeld in app-iconen, promotieafbeeldingen of video's.
- Afbeeldingen van illegaal drugsgebruik. Zelfs content voor educatieve, wetenschappelijke, artistieke of documentairedoeleinden in de winkelvermelding moet geschikt zijn voor alle leeftijden.

**Hier zijn enkele best practices:**

- Benadruk wat er zo goed is aan uw app. Deel interessante feiten over uw app zodat gebruikers begrijpen wat uw app speciaal maakt.
- Zorg dat de titel en beschrijving van uw app duidelijk de functies van uw app beschrijven.
- Gebruik geen herhaalde of irrelevante zoekwoorden of verwijzingen.
- Houd de beschrijving van uw app kort en duidelijk. Kortere beschrijvingen leiden over het algemeen tot een betere gebruikerservaring, met name op apparaten met een klein scherm. Overmatig lange of gedetailleerde beschrijvingen of beschrijvingen met een verkeerde opmaak of veel herhalingen kunnen in strijd zijn met dit beleid.
- Houd er rekening mee dat uw vermelding geschikt moet zijn voor alle leeftijden. Vermijd het gebruik van ongepaste tekst, afbeeldingen en video's in uw vermelding en houd u aan de bovenstaande richtlijnen.

## Gebruikersbeoordelingen, reviews en installaties

Ontwikkelaars mogen de plaatsing van een app op Google Play niet proberen te manipuleren. Dit omvat, maar is niet beperkt tot, het kunstmatig laten toenemen van het aantal productbeoordelingen, reviews of installaties met onrechtmatige middelen. Hieronder vallen onder andere frauduleuze reviews en beoordelingen, en reviews en beoordelingen waarvoor een beloning wordt aangeboden. Gebruikers aansporen andere apps te installeren is ook niet toegestaan als hoofddoel van de app.

We hebben normen opgesteld die content definiëren en verbieden die schadelijk of ongepast is voor onze gebruikers om ervoor te zorgen dat Google Play een veilig en respectvol platform blijft.

- Gebruikers vragen uw app te beoordelen en daarvoor een beloning aanbieden:

① Deze melding biedt gebruikers een korting in ruil voor een goede beoordeling.

- Herhaaldelijk beoordelingen indienen terwijl u zich voordoet als gebruikers om de plaatsing van een app op Google Play te beïnvloeden.

- Beoordelingen indienen (of gebruikers stimuleren om dit te doen) met ongepaste content, waaronder partners, kortingsbonnen, gamecodes, e-mailadressen of links naar websites of andere apps.

② Deze review stimuleert bezoekers om de app RescueRover te promoten door hen een kortingsbon aan te bieden.

**Beoordelingen en reviews zijn benchmarks voor de kwaliteit van een app. Gebruikers zijn afhankelijk van de authenticiteit en relevantie ervan. Hier zijn enkele best practices voor reacties op gebruikersrecensies:**

- Houd uw antwoord gericht op de problemen die in de opmerkingen van de gebruiker worden genoemd en vraag niet om een betere beoordeling.
- Vermeld verwijzingen naar nuttige hulpbronnen, zoals contactgegevens voor support of een pagina met veelgestelde vragen.

---

## Contentclassificaties

Contentclassificaties op Google Play worden geleverd door de International Age Rating Coalition (IARC) en zijn bedoeld om ontwikkelaars te helpen gebruikers op de hoogte te stellen van lokaal relevante contentclassificaties. Regionale IARC-instanties houden richtlijnen aan die worden gebruikt om het volwassenheidsniveau van de content in een app te bepalen. We staan geen apps zonder contentclassificatie toe op Google Play.

### Hoe contentclassificaties worden gebruikt

Contentclassificaties worden gebruikt om consumenten (met name ouders) te informeren over potentieel aanstootgevende content in een app. Ze helpen ook om uw content in bepaalde regio's of voor bepaalde gebruikers te filteren of te blokkeren waar dit wettelijk is vereist en om de geschiktheid van uw app voor speciale ontwikkelaarsprogramma's te bepalen.

### Hoe contentclassificaties worden toegewezen

Als u een contentclassificatie wilt ontvangen, moet u in de Play Console een vragenlijst voor classificatie invullen over de aard van de content van uw apps. Op basis van uw antwoorden op de vragenlijst wordt een contentclassificatie aan uw app toegewezen die afkomstig is van meerdere classificatie-instanties. Als u een verkeerde voorstelling van de content van uw app geeft, kan dit leiden tot verwijdering of opschorting. Het is dus belangrijk dat u correcte antwoorden opgeeft in de vragenlijst voor contentclassificatie.

U kunt voorkomen dat uw app als 'Niet geclassificeerd' wordt weergegeven door de vragenlijst voor contentclassificatie in te vullen voor elke nieuwe app die wordt ingediend bij de Play Console en voor alle bestaande apps die actief zijn op Google Play. Apps zonder contentclassificatie worden verwijderd uit de Play Store.

Als u wijzigingen aanbrengt in de content of functies van uw app die van invloed zijn op de antwoorden op de vragenlijst voor contentclassificatie, moet u een nieuwe vragenlijst voor contentclassificatie indienen via de Play Console.

Ga naar het Helpcentrum voor meer informatie over de verschillende classificatie-instanties en hoe u de vragenlijst voor contentclassificatie moet invullen.

### Bezwaar tegen een classificatie

Als u niet akkoord gaat met de contentclassificatie die aan uw app is toegewezen, kunt u rechtstreeks bezwaar indienen bij de IARC-classificatie-instantie via de link in e-mail met uw certificaat.

---

## Nieuws

Een Nieuws-app is een app die:

- gedefinieerd wordt als Nieuws-app in de Google Play Console, of
- wordt weergegeven in de categorie Nieuws en tijdschriften in de Google Play Store en zichzelf beschrijft als 'nieuws' in de titel, het icoon, de naam van de ontwikkelaar of de beschrijving van de app.

Voorbeelden van apps in de categorie Nieuws en tijdschriften die beschouwd worden als Nieuws-apps:

- Apps die zichzelf beschrijven als 'nieuws' in de app-beschrijving, inclusief maar niet beperkt tot:
  - Laatste nieuws
  - Krant
  - Actueel nieuws
  - Lokaal nieuws
  - Dagelijks nieuws
- Apps met het woord 'nieuws' in de titel, het icoon, of de naam van de ontwikkelaar van de app.

Als apps echter voornamelijk door gebruikers gegenereerde content bevatten (zoals socialmedia-apps), mogen ze niet worden gedefinieerd als Nieuws-apps en worden ze niet beschouwd als Nieuws-apps.

Nieuws-apps waarvoor een gebruiker een lidmaatschap moet aanschaffen, moeten voorafgaand aan de aankoop een in-app-contentvoorbeeld aan gebruikers bieden.

Voor Nieuws-apps geldt het volgende:

- Ze moeten eigendomsgegevens verstrekken over de app en de bron van de nieuwsartikelen, inclusief maar niet beperkt tot de oorspronkelijke uitgever of auteur van elk artikel. In gevallen waarin het niet gebruikelijk is om afzonderlijke auteurs van artikelen te vermelden, moet de Nieuws-

app de oorspronkelijke uitgever zijn van de artikelen. Links naar socialmedia-accounts zijn niet voldoende als informatie over de auteur of uitgever.
- Ze moeten beschikken over een speciale website of in-app-pagina waarvoor duidelijk is aangegeven dat deze contactgegevens bevat, die makkelijk te vinden is (bijvoorbeeld via een link onderaan de homepage of in de balk voor sitenavigatie), en die geldige contactgegevens voor de nieuwsuitgever bevat, waaronder een e-mailadres of telefoonnummer voor contact. Links naar socialmedia-accounts zijn niet voldoende als contactgegevens voor uitgevers.

Nieuws-apps mogen niet/geen:

- grote spel- en/of grammaticafouten bevatten,
- alleen statische content bevatten (bijvoorbeeld content die meer dan drie maanden oud is), of
- affiliate marketing of advertentieopbrengst als primair doel hebben.

Nieuws-apps *mogen* advertenties en andere vormen van marketing gebruiken om inkomsten te genereren, op voorwaarde dat het niet het primaire doel van de app is om producten en services te verkopen of advertentieopbrengst te genereren.

Nieuws-apps die content van verschillende publicatiebronnen verzamelen, moeten transparant zijn over de publicatiebron van de content in de app. Daarnaast moet elk van de bronnen voldoen aan de vereisten van het Nieuws-beleid.

Lees dit artikel over hoe u de vereiste informatie het beste kunt leveren.

---

## Spam en minimale functionaliteit

Apps moeten gebruikers ten minste een basisfunctionaliteit en een respectvolle gebruikerservaring bieden. Apps die crashen, ander gedrag vertonen dat niet overeenkomt met een functionele gebruikerservaring of die alleen dienen om gebruikers of Google Play te spammen, vormen geen betekenisvolle bijdrage aan onze catalogus.

## Spam

We staan geen apps toe die spam versturen naar gebruikers of naar Google Play, zoals apps die gebruikers ongewenste berichten sturen of apps die sterk lijken op andere apps of die van slechte kwaliteit zijn.

### Berichtenspam

We staan geen apps toe die sms'jes, e-mails of andere berichten namens de gebruiker versturen zonder de gebruiker de mogelijkheid te bieden de content en ontvangers goed te keuren.

We hebben normen opgesteld die content definiëren en verbieden die schadelijk of ongepast is voor onze gebruikers om ervoor te zorgen dat Google Play een veilig en respectvol platform blijft.

- Als de gebruiker op de knop Delen drukt, stuurt de app berichten uit naam van de gebruiker zonder de gebruiker de mogelijkheid te bieden de content en ontvangers goed te keuren:

## Webweergavespam en partnerspam

We staan geen apps toe die primair tot doel hebben partnerverkeer naar een website te verhogen of een webweergave te geven van een website zonder toestemming van de eigenaar of beheerder van de website.

We hebben normen opgesteld die content definiëren en verbieden die schadelijk of ongepast is voor onze gebruikers om ervoor te zorgen dat Google Play een veilig en respectvol platform blijft.

- Een app waarvan de primaire doelstelling is verwijzingsverkeer naar een website te verhogen om credits te ontvangen voor gebruikersaanmeldingen of aankopen op die website.
- Apps waarvan de primaire doelstelling is zonder toestemming een webweergave van een website te bieden.

① Deze app heet 'Ted's Shopping Deals', maar biedt alleen een webweergave van Google Shopping.

### Herhaalde content

We staan geen apps toe die slechts dezelfde functionaliteit bieden als andere apps die al aanwezig zijn op Google Play. Apps moeten waardevol zijn voor gebruikers vanwege hun unieke content of services.

We hebben normen opgesteld die content definiëren en verbieden die schadelijk of ongepast is voor onze gebruikers om ervoor te zorgen dat Google Play een veilig en respectvol platform blijft.

- Kopiëren van content uit andere apps zonder originele content of waarde toe te voegen.
- Meerdere apps maken die in functionaliteit, content en gebruikerservaring sterk op elkaar lijken. Als deze apps weinig contentvolume hebben, kunt u overwegen één app te maken met daarin alle content.

---

## Minimale functionaliteit

Zorg ervoor dat uw app een stabiele, inclusieve en responsieve gebruikerservaring biedt.

We hebben normen opgesteld die content definiëren en verbieden die schadelijk of ongepast is voor onze gebruikers om ervoor te zorgen dat Google Play een veilig en respectvol platform blijft.

- 

Apps die ontworpen zijn om niets te doen of geen functie hebben

## Defecte functionaliteit

We staan geen apps toe die crashen, geforceerd worden afgesloten, vastlopen of anderszins abnormaal functioneren.

We hebben normen opgesteld die content definiëren en verbieden die schadelijk of ongepast is voor onze gebruikers om ervoor te zorgen dat Google Play een veilig en respectvol platform blijft.

- Apps die **niet worden geïnstalleerd**
- 

Apps die worden geïnstalleerd, maar **niet worden geladen**

- Apps die worden geladen, maar **niet reageren**

## Andere programma's

Apps die zijn ontworpen voor andere Android-producten en worden gedistribueerd via Google Play, moeten niet alleen voldoen aan het inhoudsbeleid dat elders in dit Beleidscentrum is beschreven, maar kunnen ook vallen onder programmaspecifieke beleidsvereisten. Neem de onderstaande lijst door om te bepalen of een of meer van deze beleidsregels van toepassing zijn op uw app.

### Android Instant-apps

Met Android Instant-apps willen we een prettige, probleemloze gebruikerservaring bieden en tegelijkertijd voldoen aan de hoogste normen op het gebied van privacy en beveiliging. Ons beleid is ontworpen om dat doel te ondersteunen.

Ontwikkelaars die ervoor kiezen Android Instant-apps te distribueren via Google Play, moeten voldoen aan het volgende beleid, in aanvulling op al het andere programmabeleid voor ontwikkelaars van Google Play.

#### Identiteit

Voor instant-apps met inlogfunctionaliteit moeten ontwikkelaars Smart Lock voor wachtwoorden integreren.

#### Linkondersteuning

Ontwikkelaars van Android Instant-apps moeten links voor andere apps correct ondersteunen. Als de instant-apps of geïnstalleerde apps van de ontwikkelaar links bevatten die potentieel kunnen leiden naar een instant-app, moet de ontwikkelaar gebruikers naar die instant-app sturen in plaats van bijvoorbeeld de links vast te leggen in een WebView .

#### Technische specificaties

Ontwikkelaars moeten voldoen aan de technische specificaties en vereisten voor Android Instant-apps die worden geleverd door Google, die van tijd tot tijd kunnen worden aangepast, waaronder de specificaties en vereisten die worden vermeld in onze openbare documentatie .

### App-installatie aanbieden

De instant-app kan de installeerbare app aanbieden aan de gebruiker, maar dit mag niet het primaire doel van de instant-app zijn. Als installatie wordt aangeboden, is het volgende van toepassing:

- Ontwikkelaars moeten het Material Design-icoon 'app downloaden' en het label 'installeren' gebruiken voor de installatieknop.
- Ontwikkelaars mogen niet meer dan twee of drie impliciete installatieprompts opnemen in hun instant-app.
- Ontwikkelaars mogen geen banner of andere, op een advertentie lijkende techniek gebruiken om een installatieprompt aan gebruikers te presenteren.

U kunt meer informatie over instant-apps en richtlijnen voor de gebruikerservaring (UX) vinden in de praktische tips voor de gebruikerservaring .

### Apparaatstatus wijzigen

Instant-apps mogen geen wijzigingen op het apparaat van de gebruiker aanbrengen die langer van kracht zijn dan de sessie van de instant-app. Instant-apps mogen bijvoorbeeld niet de achtergrond van de gebruiker wijzigen of een widget aan het startscherm toevoegen.

### App-zichtbaarheid

Ontwikkelaars moeten ervoor zorgen dat instant-apps zichtbaar zijn voor de gebruiker, zodat de gebruiker zich ervan bewust is dat de instant-app op zijn of haar apparaat wordt uitgevoerd.

### Apparaat-ID's

Instant-apps mogen geen toegang hebben tot apparaat-ID's die (1) blijven bestaan nadat de instant-app niet meer wordt gebruikt en (2) niet kunnen worden gereset door de gebruiker. Voorbeelden hiervan zijn onder meer:

- Serienummer van build
- MAC-adressen van netwerkchips
- IMEI, IMSI

Instant-apps mogen toegang hebben tot het telefoonnummer als dit is verkregen met de runtime-machtiging. De ontwikkelaar mag niet proberen de gebruiker te identificeren aan de hand van deze ID's of andere middelen.

### Netwerkverkeer

Netwerkverkeer dat afkomstig is uit de instant-app, moet worden versleuteld met een TLS-protocol zoals HTTPS.

---

## Android-beleid voor emoji's

Ons beleid voor emoji's is ontworpen om een inclusieve en consistente gebruikerservaring te promoten. Daarom moeten alle apps de meest recente versie van Unicode-emoji's ondersteunen wanneer ze worden uitgevoerd op Android 12+.

Apps die gebruikmaken van standaard Android-emoji's zonder aangepaste implementaties, maken al gebruik van de meest recente versie van Unicode-emoji's wanneer ze worden uitgevoerd op Android 12+.

Apps met aangepaste emoji-implementaties, waaronder emoji's die worden verstrekt door bibliotheken van derden, moeten de meest recente Unicode-versie volledig ondersteunen wanneer ze worden uitgevoerd op Android 12+ binnen vier maanden na de release van nieuwe Unicode-emoji's.

Bekijk deze gids voor informatie over de ondersteuning van moderne emoji's.

Gebruik de onderstaande emoji-voorbeelden om te testen of uw app voldoet aan de nieuwste Unicode-versie:

| Voorbeelden | Unicode-versie |
|---|---|
| 🩷 🤳 🐓 | 15.0 |
| 🫠 🫱🏽 🫰🏾 | 14.0 |
| 🫩 👩🏻 👩🏿‍❤️‍👩🏿 | 13.1 |
| 🥲 🫅🏿 🐻‍❄️ | 13.0 |
| 🧑‍🦰 🚶‍♀️ 👭 | 12.1 |
| 🦩 🫃🏿 👭 | 12.0 |

# Gezinnen

Google Play heeft een uitgebreid platform waar ontwikkelaars content van hoge kwaliteit kunnen aanbieden die voor alle leeftijden geschikt is. Voordat een app wordt ingediend bij het programma Gemaakt voor gezinnen of een app die kinderen target wordt ingediend bij de Google Play Store, moet u ervoor zorgen dat uw app geschikt is voor kinderen en voldoet aan alle relevante wetgeving.

Lees meer over het proces voor gezinnen en bekijk de interactieve checklist op Academy for App Success.

## Gezinsbeleid van Google Play

Steeds meer mensen gebruiken technologie als handige aanvulling op het gezinsleven en ouders zoeken veilige content van hoge kwaliteit die ze met hun kinderen kunnen delen. Mogelijk ontwerpt u apps die specifiek voor kinderen zijn of misschien trekt uw app gewoon de aandacht van kinderen. Google Play wil u helpen ervoor te zorgen dat uw app veilig is voor alle gebruikers, inclusief gezinnen.

Het woord 'kinderen' kan verschillende betekenissen hebben in verschillende landen en in verschillende contexten. Het is belangrijk dat u contact opneemt met uw juridisch adviseur om te bepalen welke verplichtingen en/of leeftijdsbeperkingen van toepassing kunnen zijn op uw app. U weet het beste hoe uw app werkt, dus we vertrouwen erop dat u ons helpt ervoor te zorgen dat apps op Google Play veilig zijn voor gezinnen.

Alle apps die voldoen aan het Gezinsbeleid van Google Play kunnen worden aangemeld voor het programma Goedgekeurd door docenten, maar we kunnen niet garanderen dat uw app wordt opgenomen in dat programma.

## Vereisten voor Play Console

### Doelgroep en content

In het gedeelte Doelgroep en content van de Google Play Console moet u de doelgroep voor uw app aangeven voordat u deze publiceert. Dit doet u door deze te selecteren in de lijst met leeftijdsgroepen. Als u ervoor kiest afbeeldingen en terminologie op te nemen in uw app die kunnen worden beschouwd als getarget op kinderen, kan dit, ongeacht wat u aangeeft in de Google Play Console, van invloed zijn op de beoordeling van uw opgegeven doelgroep door Google Play. Google Play behoudt zich het recht voor om een eigen beoordeling uit te voeren van de app-gegevens die u verstrekt om te bepalen of de door u opgegeven doelgroep juist is.

Als u een doelgroep selecteert die alleen uit volwassenen bestaat, maar Google vaststelt dat dit onjuist is omdat uw app zowel kinderen als volwassenen target, heeft u de mogelijkheid om aan gebruikers duidelijk te maken dat uw app kinderen niet target door in te stemmen het gebruik van een waarschuwingslabel.

U mag alleen meer dan één leeftijdsgroep selecteren voor de doelgroep van uw app als u uw app heeft ontworpen voor en ervoor gezorgd heeft dat de app geschikt is voor gebruikers binnen de geselecteerde leeftijdsgroep(en). Voor apps die zijn ontworpen voor baby's, peuters en kleuters, moet bijvoorbeeld alleen de leeftijdsgroep '5 jaar en jonger' zijn geselecteerd als beoogde leeftijdsgroep voor die apps. Als uw app is ontworpen voor een specifiek klasniveau, kiest u de leeftijdsgroep die daar het best bij past. U mag alleen leeftijdsgroepen selecteren die zowel volwassenen als kinderen omvatten als u uw app daadwerkelijk heeft ontwikkeld voor alle leeftijden.

**Updates in het gedeelte 'Doelgroep en content'**

U kunt de informatie over uw app altijd updaten in het gedeelte 'Doelgroep en content' in de Google Play Console. Er is een app-update vereist voordat deze informatie wordt weergegeven in de Google Play Store. Eventuele wijzigingen die u aanbrengt in dit gedeelte van de Google Play Console kunnen echter ook voordat een app-update wordt ingediend, worden beoordeeld op naleving van het beleid.

We raden u ten zeerste aan uw bestaande gebruikers te informeren als u de getargete leeftijdsgroep van uw app wijzigt of begint met het gebruik van advertenties of in-app-aankopen. Dit kunt u doen in het gedeelte 'Wat is er nieuw' van de winkelvermeldingspagina van uw app of via meldingen in de app.

**Verkeerde voorstelling in Play Console**

Een verkeerde voorstelling van enige informatie over uw app in de Play Console, zoals in het gedeelte 'Doelgroep en content', kan ertoe leiden dat uw app wordt verwijderd of opgeschort. Het is dus belangrijk om de juiste informatie te verstrekken.

## Beleidsvereisten voor gezinnen

Als kinderen een van de doelgroepen voor uw app zijn, moet deze aan de volgende vereisten voldoen. Voldoet uw app niet aan deze vereisten, dan kan deze worden verwijderd of opgeschort.

1. **App-content:** De content van een app die voor kinderen toegankelijk is, moet geschikt zijn voor kinderen. Als uw app content bevat die niet wereldwijd gepast is, maar wel als geschikt wordt beschouwd voor gebruikers met een kinderaccount in een specifieke regio, dan kan die app beschikbaar zijn in die regio (beperkte regio's), maar blijft de app niet beschikbaar in andere regio's.
2. **App-functionaliteit:** Uw app mag niet alleen een webweergave van een webpagina bieden of het aansturen van partnerverkeer naar een website als primair doel hebben zonder toestemming van de website-eigenaar of -beheerder.
3. **Antwoorden in de Play Console:** U moet de vragen over uw app nauwkeurig beantwoorden in de Play Console en deze antwoorden updaten zodat ze eventuele wijzigingen in uw app nauwkeurig weergeven. Dit omvat, maar is niet beperkt tot, correcte antwoorden over uw app in het gedeelte Doelgroep en content, het gedeelte Veiligheid van gegevens en de IARC-vragenlijst voor contentclassificatie.
4. **Gegevensprocedures:** Als via uw app persoonlijke en gevoelige informatie van kinderen wordt verzameld, moet u dat bekendmaken, ook als dit gebeurt met behulp van API's en SDK's die in uw app worden aangeroepen of gebruikt. Gevoelige informatie over kinderen omvat, maar is niet beperkt tot, verificatie-informatie, gegevens van microfoon- en camerasensoren, apparaatgegevens, Android-ID en gebruiksgegevens voor advertenties. U moet ook zorgen dat uw app zich houdt aan de onderstaande gegevensprocedures:
   - Apps die uitsluitend kinderen targeten, mogen geen Android-advertentie-ID (AAID), serienummer van de simkaart, serienummer van de build, BSSID, MAC, SSID, IMEI en/of IMSI versturen.

    - Apps die uitsluitend kinderen targeten, mogen het recht AD_ID niet aanvragen als ze Android-API 33 of hoger targeten.
  - Apps die zowel kinderen als oudere doelgroepen targeten, mogen geen AAID, serienummer van de simkaart, serienummer van de build, BSSID, MAC, SSID, IMEI en/of IMSI versturen van kinderen of van gebruikers waarvan de leeftijd niet bekend is.
  - Het telefoonnummer van het apparaat mag niet worden opgevraagd bij de TelephonyManager van de Android-API.
  - Apps die uitsluitend kinderen targeten, mogen geen locatierechten aanvragen of de exacte locatie verzamelen, gebruiken of versturen.
  - Apps moeten de Companion Device Manager (CDM) gebruiken als ze om bluetooth verzoeken, tenzij uw app zich alleen richt op versies van het besturingssysteem die niet werken met de CDM.
5. **API's en SDK's:** U moet ervoor zorgen dat uw app eventuele API's en SDK's naar behoren uitvoert.
  - Apps die uitsluitend kinderen targeten, mogen geen API's of SDK's implementeren die niet zijn goedgekeurd voor gebruik in voornamelijk op kinderen gerichte services.
    - Denk hierbij bijvoorbeeld aan een API-service die OAuth-technologie gebruikt voor verificatie en autorisatie en waarvan de servicevoorwaarden aangeven dat de service niet is goedgekeurd voor gebruik in op kinderen gerichte services.
  - Apps die zowel kinderen als oudere doelgroepen targeten, mogen geen API's of SDK's implementeren die niet zijn goedgekeurd voor gebruik in op kinderen gerichte services, tenzij ze worden gebruikt achter een neutraal leeftijdsscherm of zodanig worden geïmplementeerd dat er geen gegevens van kinderen worden verzameld. Apps die zowel kinderen als oudere doelgroepen targeten, mogen niet vereisen dat gebruikers app-content openen via een API of SDK die niet is goedgekeurd voor gebruik in op kinderen gerichte services.

6. **Augmented Reality (AR):** Als uw app gebruikmaakt van augmented reality, moet u bij het starten van het AR-gedeelte onmiddellijk een veiligheidswaarschuwing opnemen. Deze waarschuwing moet het volgende bevatten:
  - Een geschikte melding over het belang van ouderlijk toezicht.
  - Een herinnering om zich bewust te blijven van fysieke gevaren in de echte wereld (bijvoorbeeld om zich bewust te zijn van de omgeving).
  - U mag niet vereisen dat gebruikers van uw app een apparaat nodig hebben waarvan het gebruik door kinderen wordt afgeraden (zoals Daydream of Oculus).

7. **Sociale apps en functies:** Als gebruikers via uw apps informatie kunnen delen of uitwisselen, moet u deze functies duidelijk bekendmaken in de vragenlijst voor contentclassificatie in de Play Console.
  - Sociale apps: Een sociale app is vooral bedoeld om gebruikers de mogelijkheid te geven vrijevorm-content te delen of met grote groepen mensen te communiceren. Alle sociale apps waarbij kinderen deel uitmaken van de doelgroep, moeten een in-app herinnering bieden om internet op een veilige manier te gebruiken en de risico's te begrijpen die online interactie in de echte wereld kan hebben voordat wordt toegestaan dat gebruikers met een kinderaccount vrijevorm-media of informatie uitwisselen. U moet ook verificatie door een volwassene vereisen voordat gebruikers met een kinderaccount persoonlijke informatie mogen uitwisselen.
  - Sociale functies: Een sociale functie is een aanvullende app-functionaliteit waarmee gebruikers vrijevorm-content kunnen delen of kunnen communiceren met grote groepen mensen. Elke app waarbij kinderen deel uitmaken van de doelgroep en die sociale functies bevat, moet een in-app herinnering bieden om internet op een veilige manier te gebruiken en de risico's te begrijpen die online interactie in de echte wereld kan hebben voordat wordt toegestaan dat gebruikers met een kinderaccount vrijevorm-media of informatie uitwisselen. U moet volwassenen ook een optie bieden om sociale functies voor gebruikers met een kinderaccount te beheren, inclusief maar niet beperkt tot het aan- en uitzetten van de sociale functie of het selecteren van verschillende functieniveaus. Ten slotte moet u verificatie door een volwassene vereisen voordat functies waarmee kinderen persoonlijke informatie kunnen inwisselen, worden aangezet.

- Verificatie door een volwassene is een mechanisme om te verifiëren dat de gebruiker geen kind is en kinderen niet aanmoedigt om hun leeftijd te vervalsen om toegang te krijgen tot delen van uw app die zijn bedoeld voor volwassenen (bijvoorbeeld een pincode, wachtwoord, geboortedatum, e-mailverificatie, identiteitsbewijs met foto, creditcard of SSN van een volwassene).
- Sociale apps die vooral gericht zijn op chatten met onbekende mensen, mogen geen kinderen targeten. Voorbeelden zijn onder andere chatroulette-apps, dating-apps, op kinderen gerichte openbare chatruimtes.

8. **Juridische naleving:** U moet ervoor zorgen dat uw app, inclusief eventuele API's of SDK's die uw app aanroept of gebruikt, voldoet aan de Amerikaanse Children's Online Privacy and Protection Act (COPPA) , de Algemene verordening gegevensbescherming (AVG) van de EU en eventuele andere toepasselijke wet- en regelgeving.

We hebben normen opgesteld die content definiëren en verbieden die schadelijk of ongepast is voor onze gebruikers om ervoor te zorgen dat Google Play een veilig en respectvol platform blijft.

- Apps die in de winkelvermelding spellen voor kinderen promoten, maar waarvan de app-content alleen geschikt is voor volwassenen.
- Apps die API's implementeren waarvan de servicevoorwaarden het gebruik van die API in op kinderen gerichte apps verbieden.
- Apps die het gebruik van alcohol, tabak of andere verdovende middelen idealiseren.
- Apps die echte of gesimuleerde kansspelen bevatten.
- Apps met geweld, bloedvergieten of schokkende content die niet geschikt is voor kinderen.
- Apps die datingservices leveren of seksueel of huwelijksadvies aanbieden.
- Apps die links bevatten naar websites met content die in strijd is met het Programmabeleid voor ontwikkelaars van Google Play.
- Apps die advertenties voor volwassenen tonen aan kinderen (zoals gewelddadige content, seksuele content, content over kansspelen).

## Advertenties en inkomsten genereren

Als u inkomsten genereert met een app die kinderen target op Play, is het belangrijk dat uw app voldoet aan de volgende vereisten van het Beleid voor advertenties voor gezinnen en inkomsten genereren.

Het onderstaande beleid is van toepassing op alle vormen van inkomsten genereren en adverteren in uw app, waaronder advertenties, crosspromoties (voor uw apps en apps van derden), aanbiedingen voor in-app-aankopen of andere commerciële content (zoals betaalde productplaatsing). Alle vormen van inkomsten genereren en adverteren in deze app moeten voldoen aan alle toepasselijke wet- en regelgeving (waaronder eventuele relevante zelfregulerende of brancherichtlijnen).

Google Play behoudt zich het recht voor om apps met zeer agressieve commerciële tactieken te weigeren, te verwijderen of op te schorten.

**Advertentievereisten**

Als uw app advertenties laat zien aan kinderen of aan gebruikers van een onbekende leeftijd, zorgt u voor het volgende:

- Gebruik alleen zelfgecertificeerde advertentie-SDK's voor gezinnen van Google Play om advertenties aan die gebruikers te laten zien.
- De advertenties die aan deze gebruikers worden getoond, maken geen gebruik van op interesse gebaseerd adverteren (advertenties getarget op individuele gebruikers die beschikken over bepaalde kenmerken op basis van hun online browsegedrag) of remarketing (advertenties getarget op individuele gebruikers op basis van eerdere interactie met een app of website).
- De aan deze gebruikers getoonde advertenties bevatten content die geschikt is voor kinderen.

- De aan deze gebruikers getoonde advertenties voldoen aan de vereisten voor advertentie-indeling voor gezinnen.
- Alle toepasselijke wet- en regelgeving en branchenormen die voor advertenties voor kinderen gelden, worden nageleefd.

**Vereisten voor advertentie-indelingen**

Vormen van inkomsten genereren en adverteren in uw app mogen geen misleidende content bevatten of zijn ontworpen op een manier die leidt tot onbedoelde klikken van gebruikers met een kinderaccount.

Als kinderen de enige doelgroep voor uw app zijn, is het volgende niet toegestaan. Als uw app bedoeld is voor zowel kinderen als oudere doelgroepen, is het volgende niet toegestaan wanneer u advertenties toont aan kinderen of aan gebruikers van een onbekende leeftijd:

- Storende vormen van inkomsten genereren en adverteren, waaronder vormen van inkomsten genereren en adverteren die het hele scherm vullen of het normale gebruik verstoren en geen duidelijke mogelijkheid bieden om de advertentie te sluiten (zoals advertentieblokkering).
- Vormen van inkomsten genereren en adverteren die het normale app-gebruik of de normale gameplay verstoren, waaronder advertenties met beloning of advertenties waarvoor toestemming moet worden gegeven, die niet na 5 seconden kunnen worden gesloten.
- Vormen van inkomsten genereren en adverteren die het normale app-gebruik of de normale gameplay niet verstoren, mogen langer dan 5 seconden worden getoond (bijvoorbeeld videocontent met geïntegreerde advertenties).
- Interstitial-vormen van inkomsten genereren en adverteren die onmiddellijk na het starten van de app worden getoond.
- Meerdere advertentieplaatsingen op een pagina (bijvoorbeeld banneradvertenties die meerdere aanbiedingen op één plaatsing tonen of waarin meer dan één banner of videoadvertentie wordt getoond, zijn niet toegestaan).
- Vormen van inkomsten genereren en adverteren die niet duidelijk te onderscheiden zijn van uw app-content, zoals offerwalls en andere beeldvullende advertentiebelevingen.
- Gebruik van shockerende of emotioneel manipulatieve tactieken om advertentieweergave of in-app aankopen te stimuleren.
- Misleidende advertenties die de gebruiker dwingen door te klikken met een sluitknop waarmee een andere advertentie wordt geactiveerd of met het plotseling weergeven van advertenties in gedeelten van de app waar de gebruiker meestal op een andere functie tikt.
- Geen onderscheid bieden tussen het gebruik van virtuele gamevaluta en echte valuta om in-app aankopen te doen.

We hebben normen opgesteld die content definiëren en verbieden die schadelijk of ongepast is voor onze gebruikers om ervoor te zorgen dat Google Play een veilig en respectvol platform blijft.

- Vormen van inkomsten genereren en adverteren die de vinger van de gebruiker vermijden als die ze probeert te sluiten
- Vormen van inkomsten genereren en adverteren die de gebruiker na vijf seconden geen optie bieden om de aanbieding te sluiten, zoals in het onderstaande voorbeeld:

- Vormen van inkomsten genereren en adverteren die het apparaatscherm grotendeels vullen zonder de gebruiker een duidelijke optie te geven om de advertentie te sluiten, zoals in het onderstaande voorbeeld:

- Banneradvertenties die meerdere aanbiedingen laten zien, zoals in het onderstaande voorbeeld:

- Vormen van inkomsten genereren en adverteren die door de gebruiker kunnen worden aangezien voor app-content, zoals in het onderstaande voorbeeld:

- Knoppen, advertenties of andere vormen van inkomsten genereren die uw andere winkelvermeldingen op Google Play promoten, maar die niet te onderscheiden zijn van app-content, zoals in het onderstaande voorbeeld:

**Hier volgen enkele voorbeelden van ongepaste advertentiecontent die niet mag worden getoond aan kinderen.**

- **Ongepaste mediacontent**: Advertenties voor tv-programma's, films, muziekalbums of andere mediakanalen die niet geschikt zijn voor kinderen.
- **Ongepaste videogames en downloadbare software**: Advertenties voor downloadbare software en elektronische videogames die niet geschikt zijn voor kinderen.
- **Illegale of schadelijke stoffen**: Advertenties voor alcohol, tabak, verdovende middelen en andere schadelijke stoffen.
- **Kansspelen**: Advertenties voor gesimuleerde kansspelen, wedstrijden of sweepstakes, zelfs met gratis deelname.
- **Content voor volwassenen en seksueel suggestieve content**: Advertenties met seksuele, seksueel suggestieve en niet-gezinsvriendelijke content.
- **Dating of relaties**: Advertenties voor datingsites of sites voor volwassen relaties.
- **Gewelddadige content**: Advertenties met gewelddadige en expliciete content die niet geschikt is voor kinderen.

**Advertentie-SDK's**

Als u advertenties weergeeft in uw app en uw doelgroep uitsluitend kinderen omvat, mag u alleen gebruikmaken van versies van zelfgecertificeerde advertentie-SDK's voor gezinnen . Als de doelgroep van uw app zowel uit kinderen als oudere gebruikers bestaat, moet u maatregelen voor het

checken van de leeftijd invoeren, zoals een neutraal leeftijdsscherm , en zorgen dat advertenties die aan kinderen worden getoond, uitsluitend afkomstig zijn van versies van zelfgecertificeerde advertentie-SDK's voor gezinnen van Google Play.

Bekijk de pagina met het beleid voor het Programma voor zelfgecertificeerde advertentie-SDK's voor gezinnen voor meer informatie over deze vereisten en ga naar deze pagina om de huidige lijst met versies van zelfgecertificeerde advertentie-SDK's voor gezinnen te zien.

Als u AdMob gebruikt, raadpleegt u het Helpcentrum van AdMob voor meer informatie over de producten.

Het is uw verantwoordelijkheid om ervoor te zorgen dat uw app voldoet aan alle vereisten voor advertenties, in-app aankopen en commerciële content. Neem contact op met uw aanbieder(s) van advertentie-SDK's voor meer informatie over hun contentbeleid en advertentiepraktijken.

---

## Beleid voor zelfgecertificeerde advertentie-SDK's voor gezinnen

Google Play zet zich in voor een veilige omgeving voor kinderen en gezinnen. Een belangrijk onderdeel hiervan is ervoor zorgen dat kinderen alleen advertenties te zien krijgen die geschikt zijn voor hun leeftijd en dat hun gegevens op de juiste manier worden verwerkt. Daarom vereisen we dat advertentie-SDK's en bemiddelingsplatforms zelf certificeren dat ze geschikt zijn voor kinderen en voldoen aan het Programmabeleid voor ontwikkelaars van Google Play en het Gezinsbeleid van Google Play , waaronder de vereisten van het Programma voor zelfgecertificeerde advertentie-SDK's voor gezinnen .

Met het Programma voor zelfgecertificeerde advertentie-SDK's voor gezinnen van Google Play kunnen ontwikkelaars herkennen welke advertentie-SDK's of bemiddelingsplatforms ze zelf hebben gecertificeerd als geschikt voor gebruik in apps die specifiek voor kinderen zijn ontworpen.

Een verkeerde voorstelling van informatie over uw SDK, waaronder in uw aanvraag via het interesseformulier , kan ertoe leiden dat uw SDK wordt opgeschort of verwijderd uit het Programma voor zelfgecertificeerde SDK's voor gezinnen. Het is dus belangrijk om de juiste informatie te verstrekken.

## Beleidsvereisten

Als uw SDK of bemiddelingsplatform apps levert die deel uitmaken van het Google Play-programma voor gezinnen, moet u voldoen aan het Google Play-beleid voor ontwikkelaars, waaronder aan de volgende vereisten. Als u niet voldoet aan de beleidsvereisten, kan dit leiden tot verwijdering uit of opschorting van het Programma voor zelfgecertificeerde advertentie-SDK's voor gezinnen.

U bent er verantwoordelijk voor dat uw SDK of bemiddelingsplatform voldoet aan het beleid. Zorg er daarom voor dat u het Programmabeleid voor ontwikkelaars van Google Play, het Gezinsbeleid van Google Play en de vereisten voor het Programma voor zelfgecertificeerde advertentie-SDK's voor gezinnen doorneemt.

1. **Advertentiecontent:** Uw advertentiecontent die toegankelijk is voor kinderen, moet geschikt zijn voor kinderen.
   - U moet (i) aanstootgevende advertentiecontent en aanstootgevend gedrag definiëren, en (ii) dit verbieden in uw voorwaarden of beleid. De definities moeten voldoen aan het Programmabeleid voor ontwikkelaars van Google Play.
   - Daarnaast moet u een methode ontwikkelen om uw advertentiemateriaal te classificeren voor specifieke leeftijdsgroepen. Gebruik minimaal de leeftijdsgroepen Iedereen en Volwassenen. De methode van classificatie moet overeenstemmen met de methode die Google gebruikt voor SDK's nadat het interesseformulier is ingevuld.
   - Als realtime bieden wordt gebruikt om advertenties te tonen aan kinderen, zorg dan dat het advertentiemateriaal is beoordeeld en voldoet aan de vereisten hierboven.

- Ook moet u beschikken over een mechanisme voor visuele identificatie van advertentiemateriaal uit uw voorraad (bijvoorbeeld een visueel logo van uw bedrijf als watermerk toevoegen aan het advertentiemateriaal of vergelijkbare functionaliteit).

2. **Advertentie-indeling:** U moet ervoor zorgen dat alle aan gebruikers met een kinderaccount getoonde advertenties voldoen aan de vereisten voor advertentie-indelingen voor gezinnen en u moet ontwikkelaars toestaan om advertentie-indelingen te kiezen die voldoen aan het Gezinsbeleid van Google Play.
   - Advertenties mogen geen misleidende content bevatten of zijn ontworpen op een manier die leidt tot onbedoelde klikken van gebruikers met een kinderaccount. Misleidende advertenties die de gebruiker dwingen door te klikken met een sluitknop waarmee een andere advertentie wordt geactiveerd of met het plotseling weergeven van advertenties in gedeelten van de app waar de gebruiker meestal op een andere functie tikt, zijn niet toegestaan.
   - Storende advertenties, waaronder advertenties die op het hele scherm worden getoond of die het normale gebruik verstoren en geen duidelijke manier bieden om de advertentie te sluiten (zoals advertentieblokkeringen), zijn niet toegestaan.
   - Advertenties die het normale app-gebruik of de reguliere gameplay verstoren, waaronder advertenties met beloning of advertenties waarvoor toestemming moet worden gegeven, moeten na 5 seconden kunnen worden gesloten.
   - Meerdere advertentieplaatsingen op een pagina zijn niet toegestaan. Banneradvertenties die meerdere aanbiedingen op één plaatsing tonen of waarin meer dan één banner of videoadvertentie wordt getoond, zijn niet toegestaan.
   - Advertenties moeten duidelijk te onderscheiden zijn van de content van de app. Offerwalls en beeldvullende advertenties waarvan niet meteen duidelijk is dat het gaat om advertenties voor gebruikers met een kinderaccount, zijn niet toegestaan.
   - Advertenties mogen geen gebruik maken van shockerende of emotioneel manipulatieve tactieken om advertentieweergave te stimuleren.

3. **Op interesses gebaseerd adverteren/remarketing:** U moet ervoor zorgen dat aan gebruikers met een kinderaccount getoonde advertenties niet zijn gerelateerd aan op interesses gebaseerde advertenties (advertenties die zijn getarget op individuele gebruikers met bepaalde eigenschappen op basis van hun online browsegedrag) of remarketing (advertenties die zijn getarget op individuele gebruikers op basis van eerdere interactie met een app of website).
4. **Gegevensprocedures:** U, de SDK-aanbieder, moet transparant zijn over uw verwerking van gebruikersgegevens (zoals informatie die van of over een gebruiker wordt verzameld, waaronder apparaatgegevens). Dit betekent dat u bekend moet maken tot welke gegevens uw SDK toegang heeft en hoe de SDK gegevens verzamelt, gebruikt en deelt, en dat u dit gebruik moet beperken tot de vermelde doeleinden. Deze vereisten voor Google Play gelden in aanvulling op eventuele vereisten die worden voorgeschreven in de toepasselijke wetgeving op het gebied van privacy en gegevensbescherming. U moet het aangeven als u persoonlijke en gevoelige informatie verzamelt van kinderen, inclusief, maar niet beperkt tot, verificatiegegevens, gegevens van microfoon- en camerasensoren, apparaatgegevens, Android-ID en gebruiksgegevens voor advertenties.
   - U moet ontwikkelaars toestaan om, per verzoek of per app, een behandeling als content die gericht is op kinderen aan te vragen voor de weergave van advertenties. Deze behandeling moet voldoen aan de toepasselijke wet- en regelgeving, zoals de Amerikaanse Children's Online Privacy and Protection Act (COPPA) en de Algemene verordening gegevensbescherming (AVG) van de EU .
     - Google Play vereist dat advertentie-SDK's gepersonaliseerde advertenties, op interesses gebaseerd adverteren en remarketing uitzetten als onderdeel van de behandeling als content die gericht is op kinderen.
   - Als realtime bieden wordt gebruikt om advertenties te tonen aan kinderen, moet u ervoor zorgen dat de privacyindicatoren aan de bieders bekend worden gemaakt.
   - U mag geen AAID, serienummer van de simkaart, serienummer van de build, BSSID, MAC, SSID, IMEI en/of IMSI versturen van kinderen of van gebruikers waarvan de leeftijd niet bekend is.

5. **Bemiddelingsplatforms**: U moet aan het volgende voldoen als u advertenties aan kinderen toont:
   - Gebruik alleen zelfgecertificeerde advertentie-SDK's voor gezinnen of gebruik andere waarborgen om ervoor te zorgen dat alle via bemiddeling weergegeven advertenties voldoen aan deze vereisten.
   - Geef noodzakelijke informatie door aan bemiddelingsplatforms om de classificatie voor advertentiecontent en eventueel toepasselijke behandeling als content die gericht is op kinderen aan te geven.
6. **Zelfcertificering en naleving:** U moet Google voorzien van voldoende informatie, zoals informatie die wordt vermeld in het interesseformulier , om te verifiëren of het beleid van de advertentie-SDK voldoet aan alle zelfcertificeringsvereisten, inclusief maar niet beperkt tot:
   - Een Engelstalige versie van de Servicevoorwaarden, het Privacybeleid en de Integratiegids voor uitgevers van uw SDK of bemiddelingsplatform leveren.
   - Een sample-test-app indienen die de nieuwste versie van de advertentie-SDK gebruikt die aansluit op de regelgeving. De sample-test-app moet een volledig ontwikkelde en uitvoerbare Android-APK zijn die alle functies van de SDK gebruikt. Vereisten voor test-apps:
     - De test-app moet worden ingediend als een volledige en uitvoerbare Android-APK die bedoeld is om te worden uitgevoerd op een telefoon.
     - De test-app moet de nieuwste versie of de binnenkort beschikbare versie van de advertentie-SDK gebruiken die voldoet aan het beleid van Google Play.
     - De test-app moet alle functies van uw advertentie-SDK gebruiken, waaronder het aanroepen van uw advertentie-SDK om advertenties op te halen en weer te geven.
     - De test-app moet onbeperkt toegang hebben tot de volledige advertentievoorraad voor live en weergegeven advertenties binnen het netwerk via advertentiemateriaal dat wordt aangevraagd via de test-app.
     - De toegang mag niet worden beperkt op basis van geolocatie.
     - Als uw voorraad voor een gemengde doelgroep is bedoeld, moet uw test-app onderscheid kunnen maken tussen verzoeken om advertentiemateriaal uit de volledige voorraad en uit de voorraad die geschikt is voor kinderen of alle leeftijdsgroepen.
     - De toegang mag niet worden beperkt tot specifieke advertenties in de voorraad, tenzij dit wordt beheerd door een neutraal leeftijdsscherm.
7. U moet tijdig reageren op eventuele vervolgverzoeken om informatie en door middel van zelfcertificering aangeven dat alle nieuwe versiereleases in overeenstemming zijn met het nieuwste Programmabeleid voor ontwikkelaars van Google Play, waaronder de Beleidsvereisten voor gezinnen.
8. **Juridische naleving:** Zelfgecertificeerde advertentie-SDK's voor gezinnen moeten de weergave van advertenties ondersteunen die voldoet aan alle relevante wet- en regelgeving voor kinderen die mogelijk van toepassing is op hun uitgevers.
   - U moet ervoor zorgen dat uw SDK of bemiddelingsplatform voldoet aan de Amerikaanse Children's Online Privacy and Protection Act (COPPA) , de Algemene verordening gegevensbescherming (AVG) van de EU en eventuele andere toepasselijke wet- en regelgeving.

     Opmerking: Het woord 'kinderen' kan verschillende betekenissen hebben in verschillende landen en in verschillende contexten. Het is belangrijk dat u contact opneemt met uw juridisch adviseur om te bepalen welke verplichtingen en/of leeftijdsbeperkingen van toepassing kunnen zijn op uw app. U weet het beste hoe uw app werkt, dus we vertrouwen erop dat u ons helpt ervoor te zorgen dat apps op Google Play veilig zijn voor gezinnen.

Ga naar de pagina over het Programma voor zelfgecertificeerde advertentie-SDK's voor gezinnen voor meer informatie over de Programmavereisten.

# Handhaving

Het voorkomen van een beleidsschending is altijd beter dan het beheren ervan, maar als er toch sprake is van een schending, willen we dat ontwikkelaars begrijpen hoe ze ervoor kunnen zorgen dat hun app aan het beleid voldoet. Laat het ons weten als u schendingen ziet of vragen heeft over het beheren van een schending .

## Beleidsdekking

Ons beleid is van toepassing op content die in uw app wordt weergegeven of waarnaar met links in de app wordt verwezen, advertenties die aan gebruikers worden weergegeven in de app en door gebruikers gegenereerde content die in de app wordt gehost of waarnaar wordt gelinkt. Verder is het contentbeleid van toepassing op content in uw ontwikkelaarsaccount die openbaar wordt weergegeven op Google Play, waaronder uw ontwikkelaarsnaam en de bestemmingspagina van uw vermelde ontwikkelaarswebsite.

We staan geen apps toe die gebruikers andere apps laten installeren op hun apparaat. Apps die toegang bieden tot andere apps, games of software zonder installatie, waaronder functies en functionaliteit die worden aangeboden door derden, moeten ervoor zorgen dat alle content waartoe zij toegang geven voldoet aan alle beleidsrichtlijnen van Google Play en deze apps kunnen tevens het voorwerp zijn van aanvullende beleidsreviews.

De termen die in dit beleid worden gedefinieerd, hebben dezelfde betekenis als in de distributieovereenkomst voor ontwikkelaars (DDA). De content van uw app moet niet alleen voldoen aan dit beleid en de distributieovereenkomst voor ontwikkelaars, maar moet ook worden beoordeeld op basis van onze richtlijnen voor contentclassificatie.

We staan geen apps of app-content toe die het vertrouwen van gebruikers in het Google Play-ecosysteem schaden. Als we beoordelen of we apps willen opnemen in of verwijderen uit Google Play, houden we rekening met een aantal factoren, inclusief, maar niet beperkt tot, een patroon van schadelijk gedrag of een hoog risico op misbruik. We stellen het risico op misbruik vast, inclusief, maar niet beperkt tot, items zoals klachten over specifieke apps of ontwikkelaars, nieuwsrapportage, eerdere schendingen, feedback van gebruikers en het gebruik van populaire merken, personages en andere bedrijfsmiddelen.

### Hoe Google Play Protect werkt

Google Play Protect controleert apps als u deze installeert. De functie scant ook regelmatig uw apparaat. Als er een potentieel schadelijke app wordt gevonden, kan Google Play Protect het volgende doen:

- U een melding sturen. Als u de app wilt verwijderen, tikt u op de melding en vervolgens op Verwijderen.
- De app uitschakelen totdat u deze verwijdert.
- De app automatisch verwijderen. Als er een schadelijke app wordt gedetecteerd, ontvangt u meestal een melding waarin staat dat de app is verwijderd.

#### Hoe malwarebescherming werkt

Google beschermt u tegen schadelijke software van derden, URL's en andere beveiligingsproblemen. Hiervoor kan Google informatie ontvangen over het volgende:

- De netwerkverbindingen van uw apparaat.
- Potentieel schadelijke URL's.
- Het besturingssysteem en de apps die op uw apparaat zijn geïnstalleerd via Google Play of andere bronnen.

U kunt een waarschuwing van Google ontvangen over een app of URL die mogelijk onveilig is. Als Google zeker weet dat de app schadelijk is voor apparaten, gegevens of gebruikers, kan de app of URL worden verwijderd of kan de installatie ervan worden geblokkeerd.

U kunt ervoor kiezen sommige van deze beveiligingen uit te schakelen in uw apparaatinstellingen. Google kan echter informatie blijven ontvangen over apps die zijn geïnstalleerd via Google Play. Apps die vanuit andere bronnen op uw apparaat zijn geïnstalleerd, kunnen om veiligheidsredenen nog steeds worden gecontroleerd zonder informatie naar Google te sturen.

**Hoe werken privacymeldingen?**

U krijgt een melding van Google Play Protect als een app wordt verwijderd uit de Google Play Store omdat de app toegang heeft tot uw persoonlijke informatie en u de app kunt verwijderen.

---

## Handhavingsproces

Als we content of accounts beoordelen om te bepalen of deze illegaal zijn of ons beleid schenden, baseren we onze beslissing op verschillende soorten informatie, waaronder app-metadata (bijvoorbeeld app-titel, beschrijving), in-app functionaliteit, accountgegevens (bijvoorbeeld eerdere beleidsschendingen), en andere informatie die wordt geboden via meldingsmechanismen (waar van toepassing) en reviews op eigen initiatief.

Als uw app of ontwikkelaarsaccount in strijd is met ons beleid, nemen we toepasselijke maatregelen, zoals hieronder beschreven. Daarnaast sturen we u een e-mail met relevante informatie over de genomen maatregel, samen met instructies over hoe u bezwaar kunt maken als u van mening bent dat we ten onrechte maatregelen hebben genomen.

We wijzen u erop dat verwijderings- of administratieve kennisgevingen misschien niet alle beleidsschendingen vermelden waarvan sprake is in uw account, app of app-aanbod. Ontwikkelaars zijn verantwoordelijk voor het verhelpen van beleidsproblemen en het uitvoeren van extra due diligence om te verzekeren dat de rest van de app of het account volledig aan het beleid voldoet. Als u beleidsschendingen niet in uw hele account en al uw apps verhelpt, kan dit leiden tot aanvullende handhavingsmaatregelen.

Herhaalde of ernstige schendingen (zoals malware, fraude en apps die de gebruiker of het apparaat schade kunnen toebrengen) van dit beleid of de Distributieovereenkomst voor ontwikkelaars (DDA), leiden tot de beëindiging van afzonderlijke of gerelateerde Google Play-ontwikkelaarsaccounts.

## Handhavingsmaatregelen

Verschillende handhavingsmaatregelen kunnen op verschillende manieren van invloed zijn op uw apps. We gebruiken een combinatie van menselijke en geautomatiseerde evaluaties om apps en app-content te beoordelen en content op te sporen die in strijd is met ons beleid en die schadelijk is voor gebruikers en het Google Play-ecosysteem in het algemeen. Dankzij geautomatiseerde modellen kunnen we meer schendingen opsporen en mogelijke problemen sneller evalueren. Op die manier kunnen we Google Play veilig houden voor iedereen. De content die in strijd is met het beleid kan worden verwijderd door onze geautomatiseerde modellen. In gevallen waarin een genuanceerder besluit nodig is, wordt content gemarkeerd voor verdere beoordeling door getrainde operators en analisten die contentevaluaties uitvoeren, bijvoorbeeld omdat inzicht in de context van bepaalde content nodig is. De resultaten van deze handmatige beoordelingen gebruiken we om trainingsgegevens te ontwikkelen om onze machinelearning-modellen verder te verbeteren.

In het volgende gedeelte worden de verschillende maatregelen beschreven die Google Play kan nemen en de gevolgen voor uw app en/of uw Google Play-ontwikkelaarsaccount.

Tenzij anders is aangegeven in communicatie over een handhaving, hebben deze maatregelen invloed op alle regio's. Als uw app bijvoorbeeld is opgeschort, is deze in alle regio's niet meer beschikbaar.

Daarnaast, behalve waar anders aangegeven, blijven deze maatregelen van kracht, tenzij u bezwaar maakt tegen de maatregel en het bezwaar wordt goedgekeurd.

## Afwijzing

- Een nieuwe app of app-update die ter beoordeling is ingediend, wordt niet beschikbaar gemaakt op Google Play.
- Als een update voor een bestaande app is afgewezen, blijft de app-versie die vóór de update is gepubliceerd, beschikbaar op Google Play.
- Afwijzingen hebben geen invloed op uw toegang tot de bestaande gebruikersinstallaties, statistieken en beoordelingen van een afgewezen app.
- Afwijzingen hebben geen invloed op de reputatie van uw Google Play-ontwikkelaarsaccount.

Opmerking: Probeer een afgewezen app niet opnieuw in te dienen totdat u alle beleidsschendingen heeft verholpen.

## Verwijdering

- De app en eerdere versies van de app worden verwijderd van Google Play en kunnen niet meer worden gedownload door gebruikers.
- Omdat de app is verwijderd, kunnen gebruikers de winkelvermelding van de app niet meer zien. Deze informatie wordt hersteld zodra u een beleidsconforme update indient voor de verwijderde app.
- Gebruikers kunnen mogelijk geen in-app-aankopen doen of functies voor in-app facturering in de app gebruiken totdat een beleidsconforme versie is goedgekeurd door Google Play.
- Verwijderingen hebben niet onmiddellijk invloed op de reputatie van uw Google Play-ontwikkelaarsaccount, maar meerdere verwijderingen kunnen leiden tot opschorting.

Opmerking: Probeer een verwijderde app niet opnieuw te publiceren totdat u alle beleidsschendingen heeft verholpen.

## Opschorting

- De app en eerdere versies van de app worden verwijderd van Google Play en kunnen niet meer worden gedownload door gebruikers.
- Opschorting kan plaatsvinden als gevolg van ernstige of meerdere beleidsschendingen, evenals herhaalde afwijzingen of verwijderingen van apps.
- Omdat de app is opgeschort, kunnen gebruikers de winkelvermelding van de app niet meer zien. Deze informatie wordt hersteld zodra u een beleidsconforme update indient.
- U kunt de APK of app-bundel van een opgeschorte app niet meer gebruiken.
- Gebruikers kunnen geen in-app aankopen doen of functies voor in-app facturering in de app gebruiken totdat een beleidsconforme versie is goedgekeurd door Google Play.
- Opschortingen hebben een negatief effect op de reputatie van uw Google Play-ontwikkelaarsaccount. Meerdere waarschuwingen kunnen ertoe leiden dat afzonderlijke en gerelateerde Google Play-ontwikkelaarsaccounts worden beëindigd.

Opmerking: Probeer een opgeschorte app niet opnieuw te publiceren, tenzij Google Play heeft verteld dat u dit kunt doen.

## Beperkte zichtbaarheid

- De vindbaarheid van uw app op Google Play is beperkt. Uw app blijft beschikbaar op Google Play en is toegankelijk voor gebruikers met een rechtstreekse link naar de winkelvermelding van de app.
- Als uw app de status Beperkte zichtbaarheid heeft, heeft dit geen invloed op de reputatie van uw Google Play-ontwikkelaarsaccount.

- Als uw app de status Beperkte zichtbaarheid heeft, heeft dit geen invloed op de mogelijkheid van gebruikers om de bestaande winkelvermelding van de app te bekijken.

**Beperkte regio's**

- Gebruikers kunnen uw app alleen downloaden via Google Play in bepaalde regio's.
- Gebruikers uit andere regio's kunnen de app niet vinden in de Play Store.
- Gebruikers die de app eerder hebben geïnstalleerd, kunnen deze blijven gebruiken op hun apparaat maar krijgen geen updates meer.
- Regiobeperkingen zijn niet van invloed op de reputatie van uw Google Play-ontwikkelaarsaccount.

**De status Account beperkt**

- Als uw ontwikkelaarsaccount beperkt is, worden alle apps in uw catalogus verwijderd van Google Play en kunt u geen nieuwe apps meer publiceren of bestaande apps opnieuw publiceren. U heeft nog wel gewoon toegang tot de Play Console.
- Omdat alle apps zijn verwijderd, kunnen gebruikers de winkelvermelding van uw app en uw ontwikkelaarsprofiel niet meer zien.
- Uw huidige gebruikers kunnen geen in-app aankopen doen of gebruikmaken van de functies voor in-app facturering binnen uw apps.
- U kunt nog wel de Play Console gebruiken om meer informatie aan Google Play te verstrekken en uw accountgegevens te wijzigen.
- U kunt uw apps opnieuw publiceren zodra u alle beleidsschendingen heeft verholpen.

## Beëindiging van account

- Als uw ontwikkelaarsaccount wordt beëindigd, worden alle apps in uw catalogus verwijderd van Google Play en kunt u geen nieuwe apps meer publiceren. Dit betekent ook dat eventuele gerelateerde Google Play-ontwikkelaarsaccounts permanent worden opgeschort.
- Meerdere opschortingen of opschortingen vanwege ernstige beleidsschendingen kunnen ook leiden tot de beëindiging van uw Play Console-account.
- Omdat de apps in het beëindigde account worden verwijderd, kunnen gebruikers de winkelvermelding van uw apps en uw ontwikkelaarsprofiel niet meer zien.
- Uw huidige gebruikers kunnen geen in-app aankopen doen of gebruikmaken van de functies voor in-app facturering binnen uw apps.

Opmerking: Elk nieuw account dat u probeert te openen, wordt ook beëindigd (zonder terugbetaling van de registratiekosten voor ontwikkelaars). Registreer u dus niet voor een nieuw Play Console-account als een van uw andere accounts is beëindigd.

## Slapende accounts

Slapende accounts zijn ontwikkelaarsaccounts die inactief of verlaten zijn. Slapende accounts hebben geen goede reputatie zoals vereist door de Distributieovereenkomst voor ontwikkelaars .

Google Play-ontwikkelaarsaccounts zijn bedoeld voor actieve ontwikkelaars die apps publiceren en actief onderhouden. Omdat we misbruik willen voorkomen, sluiten we regelmatig accounts die slapend zijn of die niet worden gebruikt of op een andere manier ingezet (bijvoorbeeld om apps te publiceren en te updaten, statistieken te bekijken of winkelvermeldingen te beheren).

Als uw slapende account wordt gesloten, worden het account en alle bijbehorende gegevens verwijderd. Uw registratiekosten worden niet terugbetaald en gaan verloren. Voordat we uw slapende account sluiten, stellen we u daarvan op de hoogte via de contactgegevens die u heeft opgegeven voor dat account.

Als uw slapende account wordt gesloten, kunt u in de toekomst gewoon een nieuw account maken om te publiceren op Google Play. U kunt uw account niet opnieuw activeren en eerdere apps of gegevens

zijn niet beschikbaar in een nieuw account.

---

## Beleidsschendingen beheren en melden

### Bezwaar maken tegen een handhavingsmaatregel

We herstellen apps als er een fout is gemaakt en we hebben vastgesteld dat je app het Programmabeleid van Google Play en de Distributieovereenkomst voor ontwikkelaars niet schendt. Als je het beleid zorgvuldig hebt gelezen en van mening bent dat onze beslissing onterecht is, volg je de instructies in de e-mail met de handhavingsmaatregel of klik je hier om bezwaar te maken tegen onze beslissing.

### Aanvullende bronnen

Als je meer informatie nodig hebt over een handhavingsmaatregel of een beoordeling/opmerking van een gebruiker, kun je de onderstaande bronnen raadplegen of contact met ons opnemen via het Helpcentrum van Google Play. We kunnen je echter geen juridisch advies geven. Als je juridisch advies nodig hebt, neem je contact op met je juridisch adviseur.

- App-verificatie
- Een beleidsschending melden
- Contact opnemen met Google Play over het beëindigen van een account of het verwijderen van een app
- Duidelijke waarschuwingen
- Ongepaste apps en reacties melden
- Mijn app is verwijderd van Google Play
- Uitleg van beëindiging van Google Play-ontwikkelaarsaccounts

---

### Vereisten voor de Play Console

Google Play wil gebruikers geweldige en beveiligde apps bieden en ontwikkelaars de kans geven om succesvol te zijn. We willen ervoor zorgen dat het proces om uw app beschikbaar te maken voor gebruikers zo soepel mogelijk verloopt.

Doe het volgende om veelvoorkomende schendingen te vermijden wanneer u informatie indient via de Play Console en profielen die zijn gekoppeld aan uw Play Console-ontwikkelaarsaccount.

Voordat u uw app indient:

- Verstrek nauwkeurige informatie voor uw ontwikkelaarsaccount, waaronder de volgende gegevens:
  - Officiële naam en officieel adres
  - D-U-N-S-nummer , indien u zich registreert als organisatie
  - E-mailadres en telefoonnummer voor contact
  - E-mailadres en telefoonnummer van ontwikkelaar die worden getoond op Google Play, waar van toepassing
  - Betaalmethoden, waar van toepassing
  - Het aan uw ontwikkelaarsaccount gekoppelde Google-betalingsprofiel
- Als u zich registreert als organisatie, zorg er dan voor dat de gegevens voor uw ontwikkelaarsaccount up-to-date zijn en overeenkomen met de gegevens die zijn opgeslagen in uw Dun & Bradstreet-profiel.
- Verstrek alle app-informatie en -metadata nauwkeurig
- Upload het privacybeleid van uw app en vul de vereiste items in voor het gedeelte Veiligheid van gegevens

- Verstrek een actief demo-account, inloggegevens en alle andere bronnen die nodig zijn voor Google Play om uw app te beoordelen (zoals inloggegevens, QR-code, enz.)

Zoals altijd moet u ervoor zorgen dat uw app een stabiele, aantrekkelijke en responsieve gebruikerservaring biedt. Controleer nogmaals of alles in uw app (waaronder advertentienetwerken, analyseservices en SDK's van derden) voldoet aan het Programmabeleid voor ontwikkelaars van Google Play. Als kinderen onder de doelgroep van uw app vallen, zorgt u ervoor dat uw app ook voldoet aan ons Gezinsbeleid.

Vergeet niet dat het uw verantwoordelijkheid is om de Distributieovereenkomst voor ontwikkelaars en het Programmabeleid voor ontwikkelaars na te lopen om te controleren of uw app hieraan voldoet.

Developer Distribution Agreement

Meer hulp nodig?

Probeer de volgende stappen:

**Contact opnemen**

Vertel ons meer zodat we u kunnen helpen