

Programpolicy för utvecklare (itakuwa kraft tarehe 1 Oktoba 2020)

Tillsammans bygger vi världens mest tillförlitliga källa för appar och spel

Det är utvecklarnas innovationer som ligger till grund för vår gemensamma framgång, men med det följer ansvar. Dessa programpolicyer för utvecklare i kombination med [distributionsavtalet för utvecklare](#) säkerställer att vi tillsammans kan leverera världens mest innovativa och tillförlitliga appar till över en miljard människor via Google Play. Ta del av våra policyer nedan.

Begränsat innehåll

Google Play används varje dag av personer över hela världen för att ladda ner appar och spel. Säkerställ därför att den app du skickar in är lämplig för Google Play och i enlighet med lokal lagstiftning.

Fara för barn

Appar med innehåll som sexualiserar minderåriga tas omedelbart bort från Butiken-, inklusive men inte begränsat till, appar som främjar pedofili eller olämpliga interaktioner riktade mot minderåriga (t.ex. tafsande eller smekningar).

Appar som riktar sig till barn men innehåller barnförbjudna ämnen är inte heller tillåtna, inklusive, men inte begränsat till, appar med överdrivet våld, blod och stötande innehåll och appar som skildrar eller uppmuntrar till skadliga och farliga aktiviteter. Vi tillåter inte heller appar som främjar en negativ kropps- eller självbild, inklusive appar som i underhållningssyfte skildrar plastikkirurgi, viktnedgång och andra kosmetiska förändringar av en persons fysiska utseende.

Om vi upptäcker innehåll som visar sexuellt utnyttjande av barn anmäler vi det till berörda myndigheter och tar bort Google-kontona för de som är inblandade i distributionen.

Olämpligt innehåll

I syfte att säkerställa att Google Play förblir en säker och respektfull plattform har vi skapat standarder som definierar och förbjuder innehåll som är skadligt eller opassande för våra användare.

Sexuellt innehåll och svordomar

Vi tillåter inte appar som innehåller eller marknadsför sexuellt innehåll eller svordomar, till exempel pornografi, eller innehåll och tjänster vars syfte är att vara sexuellt tilltalande. Innehåll som visar nakenhet kan vara tillåtet om det syftar till att vara utbildande, dokumentärt, vetenskapligt eller konstnärligt och inte är opåkallat.

Här är några exempel på vanliga överträdelser:

- Skildringar av sexuell nakenhet, eller sexuellt suggestiva poser där modellen är naken, oskarp eller lättklädd och/eller utstyrseln inte är acceptabel i en offentlig kontext.
- Skildringar, animationer eller illustrationer av sexuella handlingar, sexuellt suggestiva poser eller sexuella avbildningar av kroppsdelar.
- Innehåll som avbildar eller fungerar som sexuella hjälpmedel, sexualguider, olagliga sexuella teman och fetischer.
- Innehåll som är oanständigt eller anstötligt, inklusive men inte begränsat till innehåll som kan innehålla svordomar, kränkande tillmälen, explicit text, barnförbjudna/sexuella sökord i butiksuppgifterna eller i appen.
- Innehåll som avbildar, beskriver eller uppmuntrar till tidelag.
- Appar som marknadsför sexuellt relaterad underhållning, eskorttjänster eller andra tjänster som kan tolkas som att sexuella tjänster erbjuds mot betalning.
- Appar som är nedlåtande mot eller objektifierar personer.

Hatretorik

Vi tillåter inte appar som främjar våld eller som väcker hat mot individer på grund av deras etniska ursprung, religion, funktionshinder, ålder, nationalitet, veteranstatus, sexuella läggning, kön, könsidentitet eller annan egenskap som är

kopplad till systematisk diskriminering eller marginalisering.

Appar med innehåll relaterat till nazism som syftar till att vara utbildande, dokumentärt, vetenskapligt eller konstnärligt kan blockeras i vissa länder i enlighet med lokala lagar och föreskrifter.

Här är exempel på vanliga överträdelser:

- Innehåll eller retorik som hävdar att en skyddad grupp är undermänsklig, underlägsen eller förtjänar hat.
- Appar som innehåller kränkande tillmälen, stereotyper eller teorier om att en skyddad grupp uppvisar negativa särdrag (t.ex. är illvillig, korrupt eller ondskefull) eller uttryckligen eller underförstått hävdar att gruppen utgör ett hot.
- Innehåll eller retorik som försöker uppmuntra andra till att tro att individer som tillhör en skyddad grupp bör hatas eller diskrimineras.
- Innehåll som lyfter fram hatsymboler som flaggor, symboler, tecken, föremål eller beteenden med koppling till hatgrupper.

Våld

Vi tillåter inte appar som avbildar eller underlättar överdrivet våld eller andra farliga aktiviteter. Appar som skildrar fiktivt våld i ett spel, till exempel tecknat innehåll, jakt eller fiske, är i allmänhet tillåtna.

Här är några exempel på vanliga överträdelser:

- Detaljerade avbildningar eller beskrivningar av realistiskt våld eller hot om våld mot människa eller djur.
- Appar som främjar självskadebeteende, självmord, mobbning, trakasserier, ätstörningar, strypningslekar eller andra handlingar som kan leda till allvarliga skador eller dödsfall.

Terroristinnehåll

Det är inte tillåtet för terroristorganisationer att publicera appar på Google Play i något syfte, inklusive rekrytering.

Vi tillåter inte appar med innehåll kopplat till terrorism, till exempel innehåll som främjar terroristhandlingar, uppmanar till våld eller hyllar terroristattacker. Om innehåll som är relaterat till terrorism läggs upp i ett pedagogiskt, dokumentärt, vetenskapligt eller konstnärligt syfte är det viktigt att du ger tillräckligt med information så att användarna förstår sammanhanget.

Känsliga händelser

Vi tillåter inte appar vars innehåll är okänsligt mot naturkatastrofer, illdåd, konflikter, dödsfall eller andra tragiska händelser eller försöker utnyttja dessa ekonomiskt. Appar med innehåll kopplat till en känslig händelse är vanligen tillåtna om innehållet syftar till att vara utbildande, dokumentärt, vetenskapligt eller konstnärligt eller avsikten är att varna användarna för eller skapa medvetenhet kring den känsliga händelsen.

Här är exempel på vanliga överträdelser:

- Okänsligt beteende med avseende på riktiga personers eller gruppers bortgång till följd av självmord, överdos, naturliga orsaker osv.
- Förnekelse av större tragiska händelser.
- Förefalla att dra nytta av en tragisk händelse utan att detta gagnar offren på ett märkbart sätt.

Mobbning och trakasserier

Vi tillåter inte appar som innehåller eller möjliggör hot, trakasserier eller mobbning.

Här är exempel på vanliga överträdelser:

- Mobbning av offer för internationella eller religiösa konflikter.
- Innehåll vars syfte är att utnyttja andra genom bland annat utpressning.
- Att lägga upp innehåll vars syfte är att förnedra någon offentligt.
- Att trakassera offer för tragiska händelser eller deras familj och vänner.

Farliga produkter

Vi tillåter inte appar som underlättar försäljningen av sprängämnen, skjutvapen, ammunition eller vissa tillbehör för skjutvapen.

- Bland tillbehören som begränsas finns sådana som möjliggör att skjutvapen simulerar automateld, tillbehör som omvandlar ett skjutvapen till automatvapen (t.ex. fjädrande kolvar, gatling-avtryckare, automatiska avtryckare, omvandlingssatser) och magasin eller ammunitionsbälten som rymmer fler än 30 patroner.

Vi tillåter inte appar som tillhandahåller anvisningar för tillverkning av sprängämnen, skjutvapen, ammunition, begränsade skjutvapentillbehör eller andra vapen. Detta inbegriper anvisningar om hur man omvandlar ett skjutvapen till automatvapen eller simulerar automateld.

Marijuana

Vi tillåter inte appar som underlättar försäljning av marijuana eller marijuanaprodukter, oavsett laglig status.

Här är några exempel på vanliga överträdelser:

- Låter användare beställa marijuana via en kundvagnsfunktion i appen.
- Hjälper användare att ordna leverans eller upphämtning av marijuana.
- Appar som underlättar försäljning av produkter som innehåller THC (tetrahydrocannabinol), inklusive produkter som CBD-oljor med THC.

Tobak och alkohol

Vi tillåter inte appar som underlättar försäljning av tobak (inklusive e-cigarettor och vape-pennor) eller som uppmuntrar till olaglig eller olämplig användning av alkohol eller tobak.

Här är exempel på vanliga överträdelser:

- Avbildar eller uppmuntrar försäljning av alkohol eller tobak till minderåriga.
- Antyder att konsumtion av tobak kan förbättra social, sexuell, yrkesmässig, intellektuell eller idrottslig status.
- Positiva framställningar av överdrivet drickande, inbegripet positiva framställningar av måttlöst drickande, hetsdrickande eller drickande i tävlingssyfte.

Finansiella tjänster

Vi tillåter inte appar som utsätter användare för vilseledande eller skadliga finansiella produkter och tjänster.

I denna policy definierar vi finansiella produkter och tjänster som produkter eller tjänster kopplade till hantering eller investering av pengar och kryptovalutor, inklusive personlig rådgivning.

Om appen innehåller eller marknadsför finansiella produkter och tjänster måste du följa delstatliga och lokala föreskrifter för alla regioner eller länder som appen riktar sig till, såsom att inkludera specifika redogörelser som krävs enligt lokal lagstiftning.

Binära optioner

Vi tillåter inte appar som ger användarna möjlighet att handla i binära optioner.

Kryptovalutor

Vi tillåter inte appar som tillhandahåller verktyg för kryptovaluta-mining på enheter. Vi tillåter däremot appar via vilka man kan hantera kryptovaluta-mining från andra ställen.

Privatlån

Vi definierar privatlån som ett engångslån från en privatperson, en organisation eller ett rättssubjekt till en enskild konsument där syftet inte är finansiering av ett köp av en anläggningstillgång eller utbildning. Konsumenter av privatlån behöver information om kvalitet, egenskaper, avgifter, återbetalningstakt, risker och förmåner med låneprodukter för att kunna fatta välinformerade beslut om de ska ta ett lån eller inte.

- Exempel: Privatlån, snabblån, person-till-person-lån, lån med bil som säkerhet.
- Ingår inte: hypotekslån, billån, studielån, revolverande krediter (som kreditkort, personliga krediter).

Appar som erbjuder privatlån, inklusive, men inte begränsat till, appar som erbjuder lån direkt, genererar potentiella kunder och sätter konsumenter i kontakt med tredje part, måste ange följande information i appens metadata:

- Den kortaste och längsta återbetalningsperioden.
- Högsta årliga räntesats (APR), vilken oftast inkluderar ränta plus avgifter och andra kostnader under ett år eller en annan, liknande kostnad som har räknats ut i enlighet med lokal lagstiftning.
- Ett typexempel på den totala kostnaden för lånet, inklusive alla aktuella avgifter.
- En sekretesspolicy där åtkomst, insamling, användning och delning av personliga och känsliga användaruppgifter tydligt redovisas.

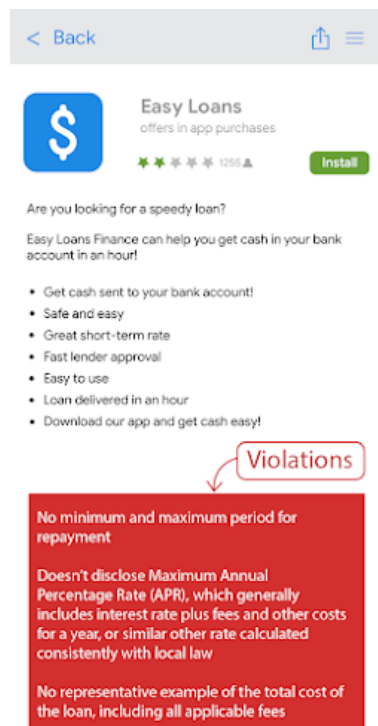
Vi tillåter inte appar som marknadsför privatlån och kräver fullständig återbetalning inom 60 dagar eller mindre från den dag lånet utfärdades (vi kallar dessa "kortsiktiga privatlån").

Privata högräntelån

I USA tillåter vi inte appar för privatlån med en årsränta (APR) på 36 % eller högre. Appar för privatlån i USA måste visa information om högsta APR, beräknad i enlighet med [Truth in Lending Act \(TILA\)](#).

Denna policy gäller appar som erbjuder lån direkt, genererar potentiella kunder och sätter konsumenter i kontakt med tredje part.

Här är ett exempel på en vanlig överträdelse:



Hasardspel, spel och tävlingar om riktiga pengar.

Vi tillåter appar med hasardspel om riktiga pengar, annonser för hasardspel om riktiga pengar och appar för daglig fantasysport som uppfyller vissa krav.

Appar med hasardspel

(Tillåts för närvarande endast i Storbritannien, Irland och Frankrike)

Vi tillåter inte appar med innehåll eller tjänster som förmedlar hasardspel på internet på några andra platser.

Vi tillåter innehåll och tjänster som förmedlar hasardspel om de uppfyller följande krav:

- Utvecklaren måste [genomgå ansökningsprocessen](#) för att distribuera appen på Play.
- Appen måste följa alla tillämpliga lagar och branschstandarder som gäller i vart och ett av de länder där den distribueras.
- Utvecklaren måste ha en giltig licens för hasardspel för varje land där appen distribueras.
- Appen måste förhindra att minderåriga användare spelar i appen.
- Appen måste förhindra användning i länder som inte omfattas av licensen för hasardspel som tillhandahålls av utvecklaren.
- Appen får INTE vara en betalapp på Google Play eller använda sig av fakturering via Google Play för köp i appar.
- Appen måste gå att ladda ned utan kostnad och installeras från Play Butik.
- Appen måste klassificeras som Endast för vuxna eller motsvarande IARC-klassificering.
- Information om ansvarsfullt spelande måste visas tydligt i appen och appinformationen.

Andra appar med spel, tävlingar och turneringar om riktiga pengar

Vi tillåter inte innehåll eller tjänster som tillåter eller underlättar att användare satsar, spelar om eller deltar med riktiga pengar (inklusive objekt i appar som köps med pengar) för att få ett pris som har ett verkligt ekonomiskt värde. Detta inkluderar men är inte begränsat till onlinekasinon, odds och lotterier som inte uppfyller de krav för hasardspelsappar som nämns ovan och spel som erbjuder kontantpriser eller annat av verkligt värde.

Här är några exempel på överträdelser:

- Spel som tar emot pengar i utbyte mot en möjlighet att vinna ett fysiskt pris eller ett pris av ekonomiskt värde.
- Spel med lojalitetspoäng (för t.ex. engagemang eller aktivitet) som (1) samlas in eller påskyndas via köp med riktiga pengar som (2) kan bytas in mot objekt eller priser av verkligt ekonomiskt värde.
- Appar som tar emot eller hanterar insatser i hasardspel, valutor i appar som krävs för deltagande, vinster eller insättningar i syfte att erhålla eller påskynda kvalificeringen för ett fysiskt pris eller ett pris av ekonomiskt värde.
- Appar som innehåller en uppmaning till handling som handlar om insatser, satsningar eller deltagande i spel, tävlingar eller turneringar om riktiga pengar, till exempel appar med navigeringselement (t.ex. menyalternativ, flikar eller knappar) som bjuder in användarna att REGISTRERA SIG eller TÄVLA i en turnering där de kan vinna ett pris i riktiga pengar.

Annonser för hasardspel eller spel, tävlingar och turneringar med riktiga pengar i appar som distribueras via Play.

Vi tillåter appar som marknadsför hasardspel eller spel, sammanhang och turneringar med riktiga pengar om de uppfyller följande krav:

- Appen och annonsen (inklusive annonsörer) måste följa alla tillämpliga lagar och branschstandarder för alla platser där annonsen visas.
- Annonsen måste uppfylla licenskraven för alla hasardspelsrelaterade produkter och tjänster som marknadsförs.
- Appen får inte visa annonser för hasardspel för individer som man vet är under 18 år.
- Appen får inte vara en del av programmet Avsett för familjer.
- Appen får inte rikta sig till individer som är under 18 år som sin primära målgrupp.
- Annonsen för en hasardspelsapp (enligt definitionen ovan) måste tydligt visa information om ansvarsfullt spelande på målsidan, i själva appinformationen eller i appen.-
- Appen får inte tillhandahålla simulerat hasardspelsinnehåll (t.ex. appar med sociala kasinon eller virtuella spelautomater).
- Appen får inte tillhandahålla stödfunktioner för hasardspel eller spel, lotterier eller turneringar om riktiga pengar (t.ex. funktioner som hjälper till med vadslagning, utbetalningar, spårning av resultat/odds eller hantering av betalningar för att delta).
- Du får inte ha äganderätt till hasardspel eller spel, lotterier eller turneringstjänster med riktiga pengar som marknadsförs i appen.
- Appinnehåll får inte marknadsföra eller hänvisa användare till hasardspel eller spel, lotterier eller turneringstjänster med riktiga pengar.

Endast appar för hasardspel (enligt definitionen ovan) eller appar som uppfyller alla dessa krav för hasardspelsannonser får innehålla annonser för hasardspel eller spel, lotterier eller turneringar med riktiga pengar.

Här är några exempel på överträdelser:

- Appar som är avsedda för minderåriga och som visar annonser som marknadsför tjänster för hasardspel.
- Simulerade kasinospel som marknadsför eller hänvisar användarna till kasinon med riktiga pengar.
- Särskilda appar för spårning av odds som innehåller integrerade annonser för hasardspel och länkar till webbplatser för sportvadslagning.
- Nyhetsappar som visar annonser för en hasardspelstjänst som ägs eller drivs av appens utvecklare.
- Appar som innehåller hasardspelsannonser som bryter mot vår policy om [vilseledande annonser](#), till exempel annonser som visas för användare i form av knappar, ikoner eller andra interaktiva element i appar

Appar med daglig fantasysport (Daily Fantasy Sports, DFS)

Vi tillåter endast appar för daglig fantasysport, enligt definitionen i tillämplig lokal lagstiftning, om de uppfyller följande krav:

- Appen måste antingen 1)-distribueras endast i USA eller 2) kvalificeras enligt ovanstående krav för hasardspelsappar.
- Utvecklaren måste genomgå processen för [ansökan om daglig fantasysport](#) och godkännas för att distribuera appen på Play.
- Appen måste följa alla tillämpliga lagar och branschstandarder som gäller i de länder där den distribueras.
- Appen måste förhindra att minderåriga satsar pengar eller genomför monetära transaktioner i appen.

- Appen får INTE vara en betalapp på Google Play eller använda sig av fakturering via Google Play för köp i appar.
- Appen måste gå att ladda ned utan kostnad och installeras från Play Butik.
- Appen måste klassificeras som Endast för vuxna eller motsvarande IARC-klassificering.
- Information om ansvarsfullt spelande måste visas tydligt i appen och appinformationen.

Om appen distribueras i USA gäller följande ytterligare krav:

- Appen måste följa alla tillämpliga lagar och branschstandarder som gäller i de amerikanska delstater eller territorier där den distribueras.
- Utvecklaren måste ha en giltig licens för var och en av de amerikanska delstaterna och territorierna där en licens krävs för appar för daglig fantasysport.
- Appen måste förhindra användning i de amerikanska delstater eller territorier där utvecklaren inte innehar den licens som krävs för appar för daglig fantasysport.
- Appar måste förhindra användning i de amerikanska delstater eller territorier där appar för daglig fantasysport inte är lagliga.

Olagliga aktiviteter

Vi tillåter inte appar som förmedlar eller marknadsför olagliga aktiviteter.

Här är några exempel på vanliga överträdelser:

- Förmedling av försäljning eller köp av olagliga droger eller receptbelagda läkemedel utan recept.
- Skildring av eller uppmuntran till användning eller försäljning av droger, alkohol eller tobak till minderåriga.
- Instruktioner för odling eller tillverkning av olagliga droger.

Användargenererat innehåll

Användargenererat innehåll är innehåll som användare bidrar med till en app och vilket är synligt eller tillgängligt för åtminstone en del av appens användare.

Appar som innehåller användargenererat innehåll måste uppfylla följande krav:

- De måste kräva att användarna godkänner appens användarvillkor och/eller användarpolicy innan användarna kan skapa eller ladda upp användargenererat innehåll.
- De måste definiera vad som utgör olämpligt innehåll och beteende (på ett sätt som uppfyller kraven i Plays programpolicy för utvecklare) och förbjuda sådant innehåll och beteende i appens användarvillkor eller användarpolicyer.
- De måste implementera kraftfull, effektiv och ständig moderering av användargenererat innehåll på ett sätt som är rimligt och överensstämmer med de typer av användargenererat innehåll som finns i appen.
 - Om livestreaming förekommer i appen måste olämpligt användargenererat innehåll tas bort så nära realtid som möjligt.
 - Om appen innehåller förstärkt verklighet (AR) måste moderering av användargenererat innehåll (inklusive rapporteringssystemet i appen) omfatta både olämpligt användargenererat innehåll i AR (t.ex. en sexuell explicit AR-bild) och känsliga ankarplatser i AR (t.ex. AR-innehåll som är förankrat till ett begränsat område, exempelvis militärbaser eller privata områden där AR-förankring kan orsaka problem för ägaren).
- Det måste finnas ett användarvänligt system i appen där det är möjligt att rapportera olämpligt användargenererat innehåll och i lämpliga fall vidta åtgärder mot användargenererat innehåll.
- Användare som trakasserar andra och bryter mot appens användarvillkor och/eller användarpolicy ska tas bort eller blockeras.
- Tillhandahåll skyddsåtgärder som förhindrar att intäktsgenerering i appen uppmuntrar användare till olämpligt beteende.

Appar vars primära syfte är att presentera stötande användargenererat innehåll tas bort från Google Play. Även appar som visar sig användas först och främst till att tillhandahålla stötande användargenererat innehåll, eller som utvecklar ett rykte bland användarna om att vara ett ställe där sådant innehåll är vanligt förekommande, tas bort från Google Play.

Här är några exempel på vanliga överträdelser:

- Främjande av sexuell explicit användargenererat innehåll, däribland genom att implementera eller tillåta betalfunktioner som främst uppmuntrar till delning av olämpligt innehåll.
- Appar med användargenererat innehåll som saknar tillräckligt skydd mot hot, trakasserier eller mobbning, framför allt mot minderåriga.
- Inlägg, kommentarer eller bilder i en app som i första hand är avsedda att trakassera eller urskilja en annan person för trakasserier, attacker eller förlöjligande.

- Appar som vid upprepade tillfällen misslyckas med att åtgärda användares klagomål om stötande innehåll.

Otillåtna ämnen

Google Play tillåter inte appar som marknadsför eller säljer otillåtna ämnen, oavsett om dessa påstås vara lagliga. Exempel:

- allt på denna icke-uttömmande lista över [förbjudna läkemedel och kosttillskott](#)
- produkter som innehåller efedra
- produkter som innehåller humant koriongonadotropin (hCG) i samband med viktminskning eller viktkontroll, eller som marknadsförs i samband med anabola steroider
- naturläkemedel och kosttillskott med aktiva farmaceutiska eller farliga ingredienser
- falska eller vilseledande hälsopåståenden, däribland påståenden som låter påskina att en produkt är lika effektiv som receptbelagda läkemedel eller kontrollerade ämnen
- produkter som inte har godkänts av myndigheterna och som marknadsförs på ett sätt som låter påskina att de är säkra eller effektiva att använda för att förhindra, bota eller behandla en viss sjukdom eller krämpa
- produkter som har varit föremål för åtgärder eller varningar från stat eller myndighet
- produkter med namn som är förvillande lika ett icke godkänt läkemedel, kosttillskott eller begränsat ämne.

Mer information om otillåtna eller vilseledande läkemedel och kosttillskott som vi granskar finns på www.legitscript.com.

Immateriell egendom

När utvecklare kopierar någon annans arbete eller använder det utan tillåtelse kan det skada ägaren av verket. Använd dig inte av andras arbete på ett otillåtet sätt.

Immateriell egendom

Vi tillåter inte appar eller utvecklarkonton som inkräktar på andras immateriella rättigheter (inklusive varumärken, upphovsrätt, patent, affärshemligheter och andra äganderättigheter). Vi tillåter heller inte appar som uppmanar eller uppmuntrar till intrång i immateriella rättigheter.

Vi vidtar åtgärder om intrång i upphovsrätten anmäls till oss. Om du vill ha mer information eller skicka en DMCA-begäran besöker du vår sida för [upphovsrättsprocesser](#).

Om du vill skicka ett klagomål gällande försäljning eller marknadsföring av förfälskade varor i en app skickar du ett [meddelande om förfälskningar](#).

Om du äger ett varumärke och anser att det finns en app på Google Play som gör intrång i varumärket rekommenderar vi att du kontaktar utvecklaren direkt för att lösa problemet. Om du inte kan nå en lösning med utgivaren skickar du ett varumärkesanspråk med det här [formuläret](#).

Om du har skriftlig dokumentation som bevisar att du har behörighet att använda immateriell egendom som tillhör en tredje part i appen eller butiksuppgifterna (t.ex. varumärkesnamn, logotyper och grafiktillgångar) [kontaktar du Google Play-teamet](#) innan du skickar in appen, så att den inte avslås på grund av intrång i immateriell egendom.

Obehörig användning av upphovsrättsskyddat material

Vi tillåter inte appar som bryter mot upphovsrätten. Att ändra upphovsrättsskyddat innehåll kan också innebära ett intrång. Utvecklare kan behöva bevisa att de har rätt att använda det upphovsrättsskyddade innehållet.

Var försiktig när du använder upphovsrättsskyddat innehåll för att visa hur din app fungerar. Oftast är det säkrast att skapa eget originalinnehåll.

Här är några exempel på upphovsrättsskyddat innehåll som ofta används utan behörighet eller ett giltigt juridiskt skäl:

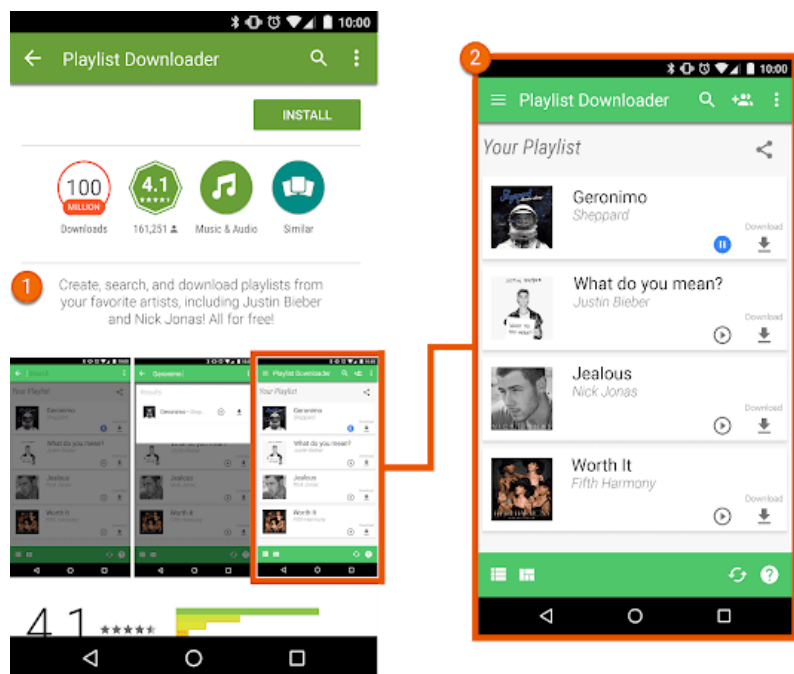
- Omslagsbilder till musikalbum, tv-spel och böcker.
- Marknadsföringsbilder från filmer, tv eller tv-spel.
- Konstverk eller bilder från serietidningar, tecknade serier, filmer, musikvideor eller tv.
- Logotyper för collegelag och proffslag.
- Bilder tagna från en offentlig persons konto på sociala medier.
- Professionella bilder av offentliga personer.
- Reproduktioner eller fan art som inte går att urskilja från upphovsrättsskyddade original.
- Appar där det spelas upp ljudklipp från upphovsrättsskyddat innehåll.
- Fullständiga reproduktioner eller översättningar av böcker som inte är allmän egendom.

Uppmuntran till intrång i upphovsrätten

Vi tillåter inte appar som uppmuntrar eller uppmanar till intrång i upphovsrätten. Fundera över om din app uppmuntrar till intrång i upphovsrätten innan du publicerar den och sök juridisk hjälp om det behövs.

Här är några exempel på vanliga överträdelser:

- Streamingappar som gör att användarna kan ladda ned en lokal kopia av upphovsrättsskyddat material utan tillåtelse.
- Appar som uppmuntrar användarna att streama och ladda ned upphovsrättsskyddat material, inklusive musik och video, i strid mot gällande upphovsrättslagstiftning.



- ① Beskrivningen i appinformationen uppmuntrar användarna att ladda ned upphovsrättsskyddat material utan tillåtelse.
- ② Skärmdumpen i appinformationen uppmuntrar användarna att ladda ned upphovsrättsskyddat material utan tillåtelse.

Varumärkesintrång

Vi tillåter inte appar som gör intrång i andras varumärken. Ett varumärke är ett ord, en symbol eller kombination som identifierar källan till en vara eller tjänst. En ägare som har förvärvat ett varumärke äger den exklusiva rätten att använda varumärket med avseende på vissa varor eller tjänster.

Varumärkesintrång är felaktig eller obehörig användning av ett identiskt eller liknande varumärke på ett sätt som kan orsaka förvirring angående källan till produkten. Om en annan parts varumärken används på ett sätt som kan orsaka förvirring i din app kan din app stängas av.

Förfalskning

Vi tillåter inte försäljning eller marknadsföring av förfälskade varor i appar. Förfälskningar har varumärken eller logotyper som är identiska med eller snarlika någon annans varumärke. De efterliknar egenskaper hos en produkt av ett visst varumärke i syfte att framstå som äkta vara från varumärkets ägare.

Sekretess, bedrägeri och otillåten användning av enheten

Det är viktigt för oss att skydda användarnas integritet och att erbjuda dem en säker miljö. Appar som är vilseledande, skadliga eller som skapats i syfte att använda nätverk, enheter eller personuppgifter på otillåtna sätt är strikt förbjudna.

Användaruppgifter

Du måste vara tydlig med hur du hanterar användaruppgifter (t.ex. uppgifter som har samlats in från eller om en användare, däribland enhetsinformation). Detta innebär att du ska uppge åtkomst, insamling, användning och delning av uppgifter i appen och begränsa användningen av uppgifterna till de syften du har angett. Om appen hanterar personliga eller känsliga användaruppgifter ska du dessutom läsa kraven i avsnittet Personliga och känsliga uppgifter nedan. Dessa krav för Google Play gäller utöver de eventuella krav som föreskrivs i tillämpliga sekretess- och dataskyddslag.

Personlig och känslig information

Personliga och känsliga användaruppgifter inbegriper, men är inte begränsade till, uppgifter som kan kopplas till en specifik individ, ekonomiska uppgifter och betalningsuppgifter, autentiseringsinformation, telefonbok, kontakter, [enhetens plats](#), uppgifter om sms och samtal, data från mikrofoner och kameror samt övrig känslig enhets- eller användningsinformation. Om appen hanterar känsliga användaruppgifter måste du göra följande:

- Begränsa åtkomsten till, insamlingen, delningen och användningen av personliga och känsliga uppgifter som har förvärvats via appen till syften som är direkt relaterade till att tillhandahålla och förbättra appens funktioner (t.ex. efterlämnade funktioner som dokumenteras och lyfts fram i appens beskrivning i Play Butik). Appar som utökar användningen av sådan data i syfte att visa annonser måste efterleva vår [annonspolicy](#).
- Lägga upp en sekretesspolicy i det avsedda fältet i Play Console och i själva appen. Sekretesspolicyn ska, tillsammans med eventuella redogörelser i appen, tydligt beskriva hur appen får åtkomst till, samlar in, använder och delar användaruppgifter. I sekretesspolicyn måste du redogöra för vilka typer av personliga och känsliga uppgifter som appen kommer åt, samlar in, använder och delar samt vilken sorts parter som personliga eller känsliga användaruppgifter delas med.
- Hantera alla användaruppgifter på ett säkert sätt, till exempel genom att överföra dem med moderna krypteringsmetoder (till exempel via HTTPS).
- Be om körningsbehörigheter om möjligt innan du kommer åt data som skyddas av [Android-behörigheter](#).
- Inte sälja personliga eller känsliga användaruppgifter.

Tydlig redogörelse och krav på samtycke

I de fall då användare inte rimligen förväntar sig att deras personliga eller känsliga användaruppgifter krävs för att tillhandahålla eller förbättra funktioner som efterlever policyn i appen (t.ex. datainsamling som sker i bakgrunden i appen) måste du uppfylla följande krav:

Du måste tillhandahålla en redogörelse i appen för hur du samlar in, använder och delar uppgifter. Redogörelsen i appen

- måste finnas i själva appen och inte bara i appbeskrivningen eller på en webbplats
- måste visas vid normal användning av appen och får inte kräva att användaren öppnar en meny eller inställningarna
- måste beskriva vilka uppgifter som appen har tillgång till eller samlar in
- måste redogöra för hur uppgifterna används och/eller delas
- får **inte** finnas enbart i en sekretesspolicy eller i användarvillkoren
- får **inte** slås ihop med andra redogörelser som inte har koppling till insamling av personliga och känsliga uppgifter.

Redogörelsen i appen måste medfölja och direkt föregå en begäran om användarens samtycke och, om möjligt, en tillhörande begäran om körningsbehörigheter. Du får inte komma åt eller samla in några personliga eller känsliga användaruppgifter innan användaren har gett sitt samtycke. En begäran om samtycke i appen måste uppfylla följande krav:

- Dialogrutan för samtycke måste visas på ett tydligt och otvetydigt sätt.
- Användaren måste ge sitt samtycke via en aktiv åtgärd (till exempel ett tryck för att godkänna eller en kryssruta som markeras).
- Om användaren navigerar bort från redogörelsen (till exempel genom att trycka på tillbakaknappen eller hemknappen) får det **inte** tolkas som samtycke.
- Meddelanden om samtycke får **inte** stängas automatiskt eller vara tidsbegränsade i syfte att få användarnas samtycke.

Här är några exempel på vanliga överträdelser:

- Appar som har åtkomst till användarens lista över installerade appar och inte behandlar dessa uppgifter som personliga eller känsliga uppgifter i enlighet med ovanstående sekretesspolicy eller kraven på datahantering, tydlig redogörelse och samtycke.
- Appar som har åtkomst till uppgifter i användarens telefon- eller kontaktbok och inte behandlar dessa uppgifter som personliga eller känsliga uppgifter i enlighet med ovanstående sekretesspolicy eller kraven på datahantering, tydlig redogörelse och samtycke.
- Om användarens skärm spelas in i appen och sådan data inte behandlas som personliga eller känsliga uppgifter i enlighet med den här policyn.
- Appar som samlar in [enhetens plats](#) utan tydlig beskrivning av hur uppgifterna används och utan att inhämta samtycke i enlighet med kraven ovan.
- Appar som samlar in begränsade behörigheter i bakgrunden i appen, inklusive i spårnings-, undersöknings- eller marknadsföringssyfte, utan tydlig beskrivning av hur uppgifterna används och utan att inhämta samtycke i enlighet med kraven ovan.

Särskilda begränsningar för åtkomst till känsliga uppgifter

Utöver de krav som beskrivs ovan gäller de krav som anges i tabellen nedan för specifika aktiviteter.

Aktivitet	Krav
Appen hanterar ekonomiska uppgifter, betalningsuppgifter, eller id-nummer som har utfärdats av en myndighet	Personliga eller känsliga användaruppgifter som är relaterade till ekonomiska uppgifter, betalningsuppgifter eller id-nummer som har utfärdats av en myndighet får inte spridas till allmänheten.
Appen hanterar telefonboks- eller kontaktuppgifter som inte är tillgängliga för allmänheten	Vi tillåter inte obehörig publicering eller spridning av andra personers kontaktuppgifter som inte är tillgängliga för allmänheten.
Appen innehåller antivirus- eller säkerhetsfunktioner, till exempel skydd mot virus, skadliga program eller säkerhetsfunktioner	Appen måste visa en sekretesspolicy som tillsammans med eventuella meddelanden i appen förklarar vilka användaruppgifter som samlas in och överförs, hur de används och med vilka parter de delas.

Privacy Shield-ramverket mellan EU och USA

Sköld för skydd av privatlivet

Om du har åtkomst till, använder eller behandlar personliga uppgifter med ursprung i EU eller Schweiz ("Personliga uppgifter inom EU") som direkt eller indirekt identifierar en individ och som har gjorts tillgängliga av Google måste du

- följa alla tillämpliga lagar, direktiv, föreskrifter och regler gällande sekretess, datasäkerhet och dataskydd
- endast ta del av, använda eller behandla Personliga uppgifter inom EU för ändamål som är förenliga med det samtycke som har inhämtats från den individ vilka dessa Personliga uppgifter inom EU avser
- vidta lämpliga organisatoriska och tekniska åtgärder i syfte att skydda Personliga uppgifter inom EU mot förlust, obehörig användning och obehörig eller olaglig åtkomst, yppande, ändringar eller förstörelse
- uppfylla skyddsnivån som krävs enligt [sekretessprinciperna för Privacy Shield](#).

Du är skyldig att regelbundet kontrollera efterlevnaden av dessa villkor. Om du vid något tillfälle inte kan uppfylla dessa villkor (eller om det finns en betydande risk att du inte kommer att kunna uppfylla dem) måste du omedelbart meddela oss via e-post på data-protection-office@google.com och antingen sluta att behandla Personliga uppgifter inom EU med omedelbar verkan eller vidta rimliga och lämpliga åtgärder för att återställa skyddet till en tillfredsställande nivå.

Behörigheter

Behörighetsförfrågningar ska vara begripliga för användarna. Du får endast begära behörigheter som krävs för att befintliga funktioner och tjänster i appen som står med i butiksuppgifterna ska kunna implementeras. Du får inte använda behörigheter som ger åtkomst till användaruppgifter eller enhetsinformation för syften som inte har uppgetts, inte har implementerats eller inte är tillåtna. Personliga och känsliga uppgifter som du får åtkomst till via behörigheter får aldrig säljas.

Begär behörighet att få åtkomst till uppgifter när de ska användas (via stegvis autentisering) så att användarna förstår varför behörigheten begärs i appen. Uppgifterna ska endast användas för de syften som användaren har gett sitt samtycke till. Om du vid ett senare tillfälle vill använda uppgifterna för andra syften måste du fråga användarna och försäkra dig om att du har deras godkännande till att använda uppgifterna för dessa ytterligare syften.

Begränsade behörigheter

I tillägg till ovanstående har begränsade behörigheter markerats med [Farlig](#), [Särskild](#) eller [Signatur](#) och omfattas av de ytterligare krav och begränsningar som följer:

- Känsliga användar- eller enhetsuppgifter som du får åtkomst till via begränsade behörigheter får endast överföras till tredje part om det är nödvändigt för att tillhandahålla eller förbättra befintliga funktioner eller tjänster i appen där uppgifterna samlades in. Du får även överföra uppgifter som nödvändigt för att efterleva tillämpliga lagar eller vid förvärv, sammanslagningar eller försäljning av tillgångar om användarna meddelas på ett juridiskt adekvat sätt. All annan överföring eller försäljning av användaruppgifter är förbjuden.
- Respektera användarnas beslut om de avvisar en begäran om begränsade behörigheter. Användarna får inte manipuleras eller tvingas att samtycka till behörigheter som inte är absolut nödvändiga. Du måste vidta rimliga åtgärder för att tillmötesgå användare som inte ger åtkomst till känsliga behörigheter (till exempel genom att låta användaren själv ange ett telefonnummer om han eller hon har nekat åtkomst till samtalsloggar).

Vissa begränsade behörigheter omfattas av ytterligare krav enligt nedan. Syftet med dessa begränsningar är att skydda användarnas integritet. Vi kan bevilja undantag från kraven nedan i begränsad utsträckning i de sällsynta fall där en app tillhandahåller en mycket användbar eller viktig funktion och det inte finns alternativa metoder för att tillhandahålla funktionen. Vi väger föreslagna undantag mot eventuell sekretess- eller säkerhetspåverkan för användarna.

Behörigheter för sms och samtalshistorik

Behörigheter för sms och samtalshistorik anses utgöra [personliga eller känsliga användaruppgifter](#) och omfattas av policyn om personliga och känsliga uppgifter och följande begränsningar:

Begränsad behörighet	Krav
Appens manifestfil behöver åtkomst till behörighetsgruppen Samtalshistorik (t.ex. <code>READ_CALL_LOG</code> , <code>WRITE_CALL_LOG</code> , <code>PROCESS_OUTGOING_CALLS</code>)	Den måste medvetet ha registrerats som standardhanteraren för telefon och assistans på enheten.
Appens manifestfil behöver åtkomst till behörighetsgruppen Sms (t.ex. <code>READ_SMS</code> , <code>SEND_SMS</code> , <code>WRITE_SMS</code> , <code>RECEIVE_SMS</code> , <code>RECEIVE_WAP_PUSH</code> , <code>RECEIVE_MMS</code>)	Den måste medvetet ha registrerats som standardhanteraren för sms och assistans på enheten.

Appar som saknar funktioner för standardhantering av sms, telefon eller assistentfunktioner får inte ange i manifestfilen att behörigheterna ovan ska användas. Detta omfattar exempeltext i manifestfilen. Appen måste dessutom medvetet ha registrerats som standardhanterare av sms, telefon eller assistentfunktioner innan användarna uppmanas att godkänna någon av ovanstående behörigheter och måste omedelbart sluta använda behörigheten när den inte längre är standardhanterare. Mer information om tillåten användning och undantag finns på [den här sidan i hjälpcentret](#).

Appar får endast använda behörigheten (och eventuella uppgifter som härrör från behörigheten) i syfte att tillhandahålla godkända grundfunktioner i appen. Med appens grundfunktion avses huvudsyftet för appen. Detta kan utgöras av en uppsättning grundfunktioner som alla måste framhållas i dokumenteringen och lyftas fram i appbeskrivningen. Utan huvudfunktionen fungerar inte appen eller blir obrukbar. Överföring, delning eller licensierad användning av dessa uppgifter får endast ske i syfte att tillhandahålla grundfunktioner eller tjänster i appen och användningen får inte utökas för något annat syfte (t.ex. för att förbättra andra appar eller tjänster eller för annonsering och marknadsföring). Du får inte använda alternativa metoder (inklusive andra behörigheter, API:er eller tredjepartskällor) för att härleda uppgifter som tillskrivs behörigheter med koppling till samtalshistoriken och sms.

Platsbehörigheter

[Enhets plats](#) anses utgöra personliga eller känsliga användaruppgifter och omfattas av policyn om [personliga och känsliga uppgifter](#) och följande krav:

- Appar får inte komma åt data som skyddas med platsbehörigheter (till exempel `ACCESS_FINE_LOCATION`, `ACCESS_COARSE_LOCATION`, `ACCESS_BACKGROUND_LOCATION`) när de inte längre krävs för att befintliga funktioner och tjänster i appen ska kunna användas.
- Du får aldrig begära platsbehörighet av användarna om annonsering eller analyser är det enda syftet. Appar som utökar den tillåtna användningen av sådan data i syfte att visa annonser måste efterleva vår [annonspolicy](#).
- Den minsta möjliga omfattningen (t.ex. ungefärlig plats i stället för exakt plats och i förgrunden i stället för i bakgrunden) som behövs för att tillhandahålla den befintliga funktionen eller tjänsten som kräver platsåtkomst ska begäras i appen och användare ska rimligen kunna anta att funktionen eller tjänsten behöver avgöra platsen med precisionen för den nivå som har begärts. Vi kan till exempel ge avslag för appar som begär eller kommer åt plats i bakgrunden utan rimligt skäl.
- Platsåtkomst i bakgrunden får endast användas för att tillhandahålla funktioner som användaren har nytta av och som hänger ihop med appens huvudfunktion.

Platsåtkomst via behörigheten för förgrunds tjänster (när appen bara har platsåtkomst i förgrunden, t.ex. medan appen används) är tillåten om användningen

- har inletts som en direkt följd av en användarinitierad åtgärd i appen
- avslutas omedelbart när det avsedda användningsfallet för den användarinitierade åtgärden har slutförts i appen.

Appar som särskilt riktar sig till barn måste följa policyn för [Avsett för familjer](#).

Behörigheten Åtkomst till alla filer

Filer och katalogattribut på användarnas enheter anses utgöra personliga eller känsliga användaruppgifter och omfattas av policyn om [personliga och känsliga uppgifter](#) och följande krav:

- Appar bör endast begära åtkomst till det lagringsutrymme på enheten som är avgörande för att appen ska fungera och får inte begära åtkomst till enhetens lagringsutrymme på uppdrag av tredje part för något ändamål som inte har någon koppling till appfunktioner som visas för användaren.
- Android-enheter som kör R (Android 11, API-nivå 30) eller senare måste ha behörigheten [MANAGE_EXTERNAL_STORAGE](#) för att hantera åtkomst i delad lagring. Alla appar som är inriktade på R och begär bred åtkomst till delad lagring (Åtkomst till alla filer) måste godkännas i en lämplig åtkomstgranskning innan de publiceras. Appar som tillåts använda denna behörighet måste tydligt uppmana användarna att aktivera Åtkomst till alla filer för appen under inställningarna Särskild appåtkomst. Du hittar mer information om kraven för R i den här hjälpartikeln.

Otillåten användning av enheter och nätverk

Vi tillåter inte appar som stör, skadar eller på ett otillåtet sätt får åtkomst till användarens enhet, andra enheter eller datorer, servrar, nätverk, programmeringsgränssnitt (API:er) eller tjänster, inklusive men utan begränsning till andra appar på enheten, Googles tjänster eller en auktoriserad operatörs nätverk.

Alla appar på Google Play måste följa systemoptimeringskraven för Android som beskrivs i [riktlinjerna för grundläggande appkvalitet för Google Play](#).

En app som distribueras via Google Play får inte ändra, ersätta eller uppdatera sig själv med någon annan metod än Google Plays uppdateringsfunktion. Dessutom får enbart körbar kod (t.ex. filformaten dex, JAR och .so) från Google Play laddas ned av en app. Denna begränsning gäller inte för kod som körs i en virtuell dator och som har begränsad tillgång till Android API (till exempel JavaScript i WebView eller webbläsare).

Vi tillåter inte kod som introducerar eller utnyttjar säkerhetsbrister. Kolla in programmet [Förbättring av appsäkerhet](#) om du vill veta mer om de senaste säkerhetsproblemen som har flaggats för utvecklare.

Här är några exempel på vanliga överträdelser:

- Appar som blockerar eller stör en annan app som visar annonser.
- Fuskappar som påverkar spelet i andra appar.
- Appar som förmedlar eller ger instruktioner om hur man hackar tjänster, programvara eller maskinvara, eller hur man kringgår säkerhetsskydd.
- Appar som får åtkomst till eller använder en tjänst eller ett API på ett sätt som bryter mot dess användarvillkor.
- Appar som inte [uppfyller kraven för godkännande](#) och försöker kringgå [systemets strömhantering](#).
- Appar som underlättar proxytjänster till tredje part får endast göra så om detta är appens primära och grundläggande syfte som visas för användarna.
- Appar eller kod från tredje part (t.ex. SDK:er) där körbar kod, till exempel dex-filer och plattformsspecifik kod, laddas ned från en annan källa än Google Play.
- Appar som installerar andra appar på en enhet utan användarens föregående samtycke.
- Appar som länkar till eller förmedlar distribution eller installation av skadlig programvara.

Vilseledande funktioner

Vi tillåter inte appar som försöker vilseleda användare eller möjliggör ohederligt beteende. Detta omfattar men är inte begränsat till appar som bedöms innehålla funktioner som är tekniskt omöjliga. Appar ska ha en korrekt redogörelse, beskrivning och bilder eller video av hur funktionerna fungerar i alla delar av metadatan. Appar får inte imitera funktioner eller varningar från operativsystem eller andra appar. Eventuella ändringar i enhetsinställningar måste göras med användarens vetskap och samtycke och kunna återställas av användaren.

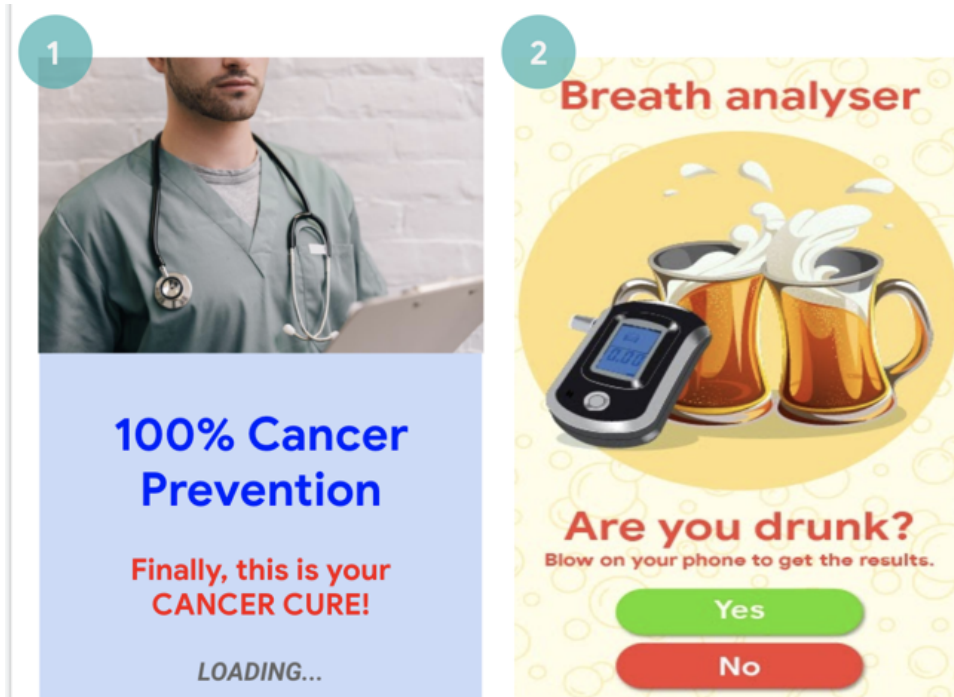
Vilseledande påståenden

Vi tillåter inte appar som innehåller falska eller vilseledande uppgifter eller påståenden i appens beskrivning, titel, ikon, skärmdumpar och så vidare.

Här är några exempel på vanliga överträdelser:

- Appar som framställer sina funktioner på ett missvisande eller otydligt sätt:
 - En app som påstås vara ett racingspel i beskrivningen och skärmdumparna, men i själva verket är ett pusselspel med en bild av en bil.
 - En app som påstås vara en antivirusapp, men som bara innehåller en textbeskrivning av hur virus kan tas bort.
- Namn på utvecklare eller appar som på ett felaktigt sätt anger sin aktuella status eller resultat på Play. (T.ex. "Redaktionens val", "Bästa appen", "Storsäljare").
- Appar med medicinska eller hälsorelaterade funktioner och innehåll som är vilseledande eller potentiellt skadliga.

- Appar som utges för att ha funktioner som är omöjliga att implementera (t.ex. appar som stöter bort insekter) även om detta presenteras som spratt, skämt, falskt, etc.
- Appar som är felaktigt kategoriserade, inklusive men inte begränsat till appens klassificering eller appkategori.
- Bevisligen vilseledande innehåll som kan påverka röstningsprocesser.
- Appar som felaktigt påstås ha anknytning till en myndighet eller tillhandahålla eller förmedla myndighetstjänster som appen inte har auktoriserats för.
- Appar som felaktigt utges för att vara officiella appar för etablerade rättssubjekt. Titlar som Justin Bieber Official får inte användas utan tillåtelse eller rättigheter.



- (1) Denna app innehåller medicinska eller hälsorelaterade påståenden (Bota cancer) som är vilseledande
 (2) Appen utges för att ha funktioner som är omöjliga att implementera (att du kan använda telefonen som alkoholmätare)

Vilseledande ändringar av enhetsinställningar

Vi tillåter inte appar som gör ändringar i användarens enhetsinställningar eller funktioner utanför appen utan användarens vetskap och samtycke. Enhetsinställningar och enhetsfunktioner omfattar systemets och webbläsarens inställningar, bokmärken, genvägar, ikoner, widgetar och visningen av appar på startskärmen.

Vi tillåter inte heller:

- Appar som ändrar enhetsinställningar eller enhetsfunktioner med användarens samtycke, men på ett sätt som inte är lätt att återställa.
- Appar eller annonser som ändrar enhetens inställningar eller funktioner som en tjänst till tredje part eller i annonseringssyfte.
- Appar som vilseleder användarna för att få dem att ta bort eller inaktivera tredje parts appar eller ändra enhetsinställningar eller enhetsfunktioner.
- Appar som uppmuntrar eller sporrar användarna till att ta bort eller inaktivera appar från tredje part eller ändra enhetsinställningar eller enhetsfunktioner. Detta gäller inte för verifierbara säkerhetstjänster.

Möjliggöra ohederligt beteende

Vi tillåter inte appar som hjälper användare att vilseleda andra eller innehåller funktioner som är bedrägliga på något sätt. Detta omfattar men är inte begränsat till appar som skapar eller underlättar skapande av id-kort, personnummer, pass, examensbevis, kreditkort eller körkort. Appar ska ha en korrekt redogörelse, titel, beskrivning och bilder eller video av appens funktioner och/eller innehåll och ska fungera på ett sätt som användaren har rimlig anledning att förvänta sig.

Ytterligare appresurser (till exempel speltillgångar) får endast laddas ned om användaren annars inte kan fortsätta att använda appen. Resursnedladdningar måste efterleva alla Google Plays policyer. Före nedladdningen ska användarna meddelas i appen och nedladdningsstorleken tydligt meddelas.

Påståenden om att en app är en skämtapp eller ska användas i underhållningssyfte (eller annat synonymt uttryck) undantar inte appen från våra policyer.

Här är några exempel på vanliga överträdelser:

- Appar som imiterar andra appar eller webbplatser för att lura användare att avslöja personuppgifter eller autentiseringsinformation.
- Appar som utan samtycke visar överifierade eller riktiga telefonnummer, kontakter eller adresser till personer eller rättssubjekt eller uppgifter som kan kopplas till en specifik individ eller ett specifikt rättssubjekt.
- Appar som har olika huvudfunktioner baserat på var användarna bor, enhetsparametrar eller annan användarberoende data och inte tydligt tillkännager dessa skillnader för användaren i butiksuppgifterna.
- Appar som ändras på ett betydligt sätt mellan olika versioner utan att förvarna användaren (t.ex. [avsnittet Nyheter](#)) och uppdaterar butiksuppgifterna.
- Appar som försöker ändra eller obfuskerar funktioner under granskningen.
- Appar där ett nätverk för innehållsleverans (NFI) används för nedladdningar men användaren inte meddelas eller informeras om nedladdningsstorleken före nedladdningen.

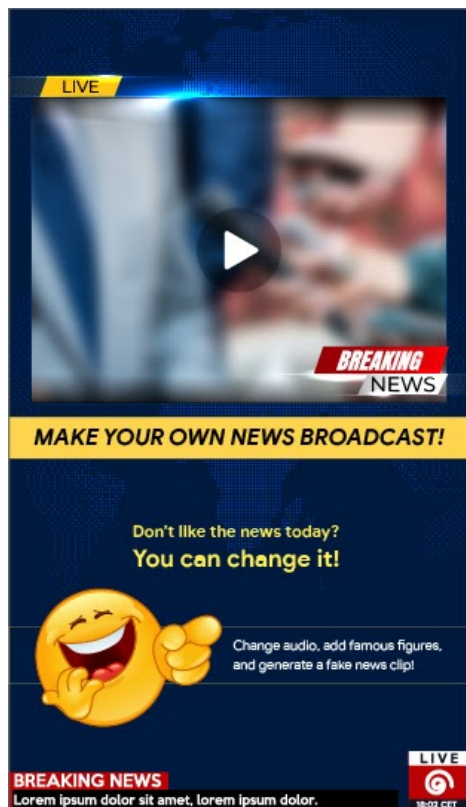
Manipulerad media

Vi tillåter inte appar som främjar eller skapar falsk eller vilseledande information eller påståenden med hjälp av bilder, videor och/eller text. Vi tar bort appar som anses främja eller sprida bevisligt vilseledande eller bedrägliga bilder, videor och/eller texter som kan vara skadliga med avseende på känsliga händelser, politik, sociala frågor eller annat som är av intresse för allmänheten.

Appar som manipulerar eller förändrar media utöver vedertagna och redaktionella klarhets- och kvalitetsjusteringar måste tydligt meddela eller vattenstämpla manipulerad media om det kanske inte framgår för vanliga människor att den har förändrats. Undantag kan ges för media som är av intresse för allmänheten eller uppenbar satir eller parodi.

Här är några exempel på vanliga överträdelser:

- Appar som lägger till en offentlig person i en demonstration vid en politiskt känslig händelse.
- Appar som använder offentliga personer eller media från en känslig händelse i syfte att marknadsföra funktioner för att manipulera media i appens butiksuppgifter.
- Appar som manipulerar medieklipp för att efterlikna en nyhetssändning.



(1) Denna app tillhandahåller en funktion för att manipulera medieklipp i syfte att efterlikna en nyhetssändning och lägger till berömda eller offentliga personer i klippet utan en vattenstämpel.

Felaktig framställning

Vi tillåter inte appar eller utvecklarkonton i annan persons eller organisations namn eller som döljer eller felaktigt framställer ägarens identitet eller vad det primära syftet är. Vi tillåter inte appar eller utvecklarkonton som ägnar sig åt samordnade aktiviteter i syfte att vilseleda användare. Detta innebär men är inte begränsat till appar och utvecklarkonton som döljer eller felaktigt framställer sitt ursprungsland och som riktar innehåll till användare i ett annat land.

Skadlig programvara

All kod som kan utgöra en risk för användare, användarnas data eller enheter räknas som skadlig programvara. Skadlig programvara omfattar men är inte begränsat till potentiellt skadliga appar, binärfiler eller modifiering av ramverk inom kategorier som trojaner, nätfiske och spionprogram. Vi uppdaterar ständigt listan och lägger till nya kategorier.

Skadlig programvara

Vår policy om skadlig programvara är enkel: ingen skadlig programvara ska finnas på Google Play Butik, i användarnas enheter eller resten av Androids ekosystem. Utifrån denna grundläggande princip strävar vi efter att Androids ekosystem ska vara säkert för användarna och deras Android-enheter.

Skadlig programvara kan vara av olika typer eller ha skilda funktioner, men målet är oftast ett av följande:

- Få tillgång till användarens enhet.
- Få kontroll över användarens enhet.
- Aktivera fjärrstyrda åtgärder så att angriparen kan komma åt, använda eller på annat sätt utnyttja den infekterade enheten.
- Överföra personuppgifter eller användaruppgifter från enheten utan tydlig redogörelse och utan samtycke.
- Sprida skräppost eller ge kommandon från den infekterade enheten i syfte att påverka andra enheter eller nätverk.
- Utsätta användaren för bedrägeri.

Det finns potentiellt skadliga appar, binärfiler och modifieringar för ramverk. Dessa kan vara oavsiktligt skadliga. Detta beror på att appar, binärfiler och modifieringar för ramverk kan fungera på olika sätt utifrån olika variabler. Därför kan något vara skadligt på en Android-enhet men inte utgöra någon risk alls på en annan. Om till exempel en enhet har den senaste versionen av Android påverkas den inte av skadliga appar som utnyttjar utfasade API:er, medan en enhet som fortfarande använder en tidigare version av Android kan utsättas för fara. Appar, binärfiler och modifieringar för ramverk flaggas som skadliga eller potentiellt skadliga om de utgör en tydlig risk för vissa eller alla Android-enheter och -användare.

Det är viktigt för oss att användarna ska förstå hur deras enhet används samt att ekosystemet är både säkert och har utrymme för både innovation och en trygg användarupplevelse. Det är grundstenen för kategorierna för skadlig programvara nedan.

Besök [Google Play Protect](#) om du vill veta mer.

Bakdörrar

Kod som möjliggör att oönskade eller potentiellt skadliga fjärrstyrda åtgärder utförs på en enhet.

Dessa åtgärder kan omfatta beteenden som skulle placera appen, binärfilen eller modifieringen av ramverket i en av de andra kategorierna för skadlig programvara om de utfördes automatiskt. Ordet bakdörr används i allmänhet som en beskrivning av hur en potentiellt skadlig åtgärd kan ske på en enhet och stämmer därför inte helt överens med kategorier som faktureringsbedrägeri eller kommersiella spionprogram. Därför kan bakdörrar under vissa omständigheter behandlas som säkerhetsbrister i Google Play Protect.

Faktureringsbedrägeri

Kod som automatiskt debiterar användaren på ett avsiktligt bedrägligt sätt.

Bedrägeri via mobilräkningen delas in i sms-bedrägeri, samtalsbedrägeri och avgiftsbedrägeri.

Sms-bedrägeri

Kod som debiterar användare för betal-sms som skickats utan samtycke eller som försöker dölja sms-aktiviteter genom att gömma avtal eller sms från mobiloperatören där användaren aviseras om avgifter eller får bekräftelse på prenumerationer.

Viss kod introducerar ytterligare funktioner som möjliggör sms-bedrägeri, även om den tekniskt informerar om att sms skickas. Det kan till exempel innebära att delar av ett avtal döljs från användaren och blir oläsliga eller att sms från

mobiloperatören till användaren med avisering om avgifter eller bekräftelse på prenumerationer under vissa förutsättningar inte visas.

Samtalsbedrägeri

Kod som debiterar användare genom att ringa till betalnummer utan användarens samtycke.

Avgiftsbedrägeri

Kod som lurar användare till att prenumerera på eller köpa innehåll via mobilräkningen.

I avgiftsbedrägeri ingår all typ av fakturering med undantag för betal-sms och betalsamtal. Några exempel är direktdebitering via operatören, trådlös åtkomstpunkt (WAP) och överföring av telefonens saldo. Bedrägeri relaterat till WAP tillhör den vanligaste formen av avgiftsbedrägeri. Användare kan luras till att klicka på en knapp på en transparent WebView som lästs in i bakgrunden. När åtgärden utförs startar en återkommande prenumeration, och bekräftelsemeddelandet kapas ofta så att användare inte ska upptäcka den ekonomiska transaktionen.

Förföljelseprogram

Kod som överför personliga uppgifter från enheten utan tydlig avisering och utan samtycke och som inte visar en beständig avisering om att detta händer.

Appar med förföljelseprogram överför vanligtvis data till andra än leverantören av de potentiellt skadliga apparna.

Godkända former av sådana appar används till exempel av föräldrar som vill se var deras barn befinner sig. Dessa appar kan användas för att spåra någon (till exempel en partner) utan personens vetskap eller tillåtelse såvida inte en beständig avisering visas medan data överförs.

Endast appar som uppfyller kraven i våra policyer och som har utformats och marknadsförts för föräldrakontroll (inklusive familjeadministration) eller företagshantering får distribueras med spårnings- och rapportfunktioner i Play Butik, förutsatt att de uppfyller alla ovanstående krav.

Appar som inte är förföljelseprogram som distribueras i Play Butik och som övervakar eller följer en användares beteende på en enhet måste följa dessa krav:

- Appar får inte presenteras som lösningar för spioneri eller hemlig övervakning.
- Appar får inte dölja spårningsbeteende eller försöka vilseleda användare om sådana funktioner.
- Apparna måste visa en beständig avisering och en unik ikon som tydligt identifierar appen för användarna.
- Appar och appuppgifter på Google Play får inte innehålla funktioner som aktiverar eller ger åtkomst till funktioner som bryter mot dessa villkor, till exempel länkar till APK utanför Google Play som inte följer villkoren.
- Du är själv ansvarig för att avgöra om appen är laglig i det land eller på den plats där den finns tillgänglig. Appar som finns vara olagliga på platser där de publiceras tas bort.

Överbelastningsattack (DoS)

Kod som, utan användarens vetskap, utför en överbelastningsattack (DoS) eller är en del av en distribuerad överbelastningsattack mot andra system och resurser.

Detta kan till exempel ske genom att ett stort antal HTTP-förfrågningar skickas i syfte att åstadkomma mycket hög belastning på fjärrservrar.

Fientliga nedladdare

Kod som i sig inte är potentiellt skadlig men som laddar ned andra appar som är det.

Koden kan vara en fientlig nedladdare om

- det finns skäl att misstänka att den skapats för att sprida potentiellt skadliga appar och har laddat ned sådana appar eller om den innehåller kod som kan ladda ned och installera appar eller
- minst 5 % av de appar som den har laddat ned är potentiellt skadliga appar med en lägsta gräns på 500 faktiska nedladdningar (25 faktiska nedladdningar av potentiellt skadliga appar).

Större webbläsare och fildelningsappar betraktas inte som fientliga nedladdare så länge som

- de inte inleder nedladdningar utan interaktion med användaren, och
- alla nedladdningar av potentiellt skadliga appar initieras av användare som samtycker.

Hot som inte drabbar Android

Kod som innehåller hot som inte drabbar Android.

Dessa appar är inte skadliga för Android-enheter eller Android-användare, men de har komponenter som kan vara skadliga på andra plattformar.

Nätfiske

Kod som utges för att komma från en betrodd källa, begär åtkomst till användarens autentiserings- eller faktureringsuppgifter och skickar datan till tredje part. Den här kategorin omfattar även kod som kapar användaruppgifter när de skickas.

Målet med nätfiske är att komma över bland annat användaruppgifter till banktjänster, kreditkortsnummer och kontouppgifter för sociala nätverk och spel online.

Otillåten användning av eskalerade behörigheter

Kod som får tillgång till systemet genom att skada appens sandlåda, ändra eller inaktivera åtkomsten till viktiga säkerhetsfunktioner eller skaffa sig högre behörigheter.

Exempel:

- Appar som inte följer Androids behörighetsmodell eller stjälar användaruppgifter (till exempel OAuth-token) från andra appar.
- Appar som utnyttjar funktioner på otillåtna sätt så att det inte går att stoppa eller avinstallera dem.
- Appar som inaktiverar SELinux.

Appar som eskalerar behörigheter för att kunna roota enheter utan användarens tillstånd klassificeras som rootningsappar.

Utpressningsvirus

Kod som delvis eller fullständigt tar kontroll över en enhet eller data på en enhet och kräver att användaren betalar eller utför åtgärder för att få tillbaka kontrollen.

En del utpressningsvirus krypterar data på enheten och kräver betalning i utbyte mot att datan dekrypteras och/eller utnyttjar administratörsfunktioner så att viruset inte kan tas bort av den genomsnittliga användaren. Exempel:

- Låser användaren ute från enheten och kräver pengar i utbyte mot att ge tillbaka kontrollen.
- Krypterar data på enheten och kräver betalning, till synes i utbyte mot att dekryptera datan.
- Utnyttjar funktioner för att hantera policyer för enheten och omöjliggöra borttagning av användaren.

Kod som distribueras tillsammans med enheten vars huvudsyfte är att minska enhetshanteringen kan undantas från utpressningsviruskategorin om den uppfyller kraven om säker låsning och hantering, samtycke samt tydligt informerar användaren.

Rootning

Kod som rootar enheten.

Det är skillnad på icke-skadlig och skadlig rootningskod. Icke-skadliga rootningsappar informerar exempelvis användaren innan de rootar enheten, och de utför inga andra av de potentiellt skadliga åtgärderna i de övriga kategorierna.

Skadliga rootningsappar meddelar inte användaren att enheten är på väg att rootas, eller så meddelar de användaren om rootningen i förväg men utför även andra åtgärder som hör hemma i samma kategori som andra potentiellt skadliga appar.

Spam

Kod som skickar oönskade meddelanden till användarens kontakter eller förvandlar enheten till ett skräppostrelä.

Spionprogram

Kod som överför personuppgifter från enheten utan tydligt meddelande och utan samtycke.

Om till exempel något av följande överförs utan redogörelse eller på ett för användaren oväntat sätt klassas koden som spionprogram:

- Kontaktlistor

- Foton eller andra filer som inte ägs av appen eller som överförs från SD-kortet
- Innehåll från användarens e-postkonto
- Samtalshistorik
- Sms-loggar
- Webbhistorik eller bokmärken från standardwebbläsaren
- Information från katalogerna /data/ i andra appar

Allt spionage på användaren kan flaggas som spionprogram. Till exempel om ljud eller samtal på telefonen spelas in eller appdata stjäls.

Trojan

Kod som verkar vara genuin, till exempel ett spel som utges för att bara vara ett spel, men som utför oönskade åtgärder mot användaren.

Den här klassificeringen används oftast tillsammans med andra kategorier för potentiella skadliga appar. En trojan har en harmlös komponent och en skadlig, dold komponent. Till exempel ett spel som skickar avgiftsbelagda sms från enheten i bakgrunden utan användarens vetskap.

Information om ovanliga appar

Nya och unika appar kan klassificeras som ovanliga om det inte finns tillräcklig information för att säkerställa att de är säkra i Google Play Protect. Detta innebär inte nödvändigtvis att appen är skadlig, bara att den behöver granskas närmare för att säkerställa att den är säker.

Information om bakdörrskategorin

Klassificeringen för kategorin om programvara som är skadlig på grund av en bakdörr beror på hur koden fungerar. Ett villkor för att koden ska klassas som en bakdörr är att den möjliggör beteenden som skulle placera koden i en av de andra kategorierna för skadlig programvara om den kördes automatiskt. Om till exempel dynamisk kod kan läsas in i appen och sms samlas in med hjälp av den dynamiskt inlästa koden klassificeras den som programvara som är skadlig på grund av en bakdörr.

Om godtycklig kod kan köras i appen och vi inte har någon anledning att tro att koden har lagts till i skadesyfte kan däremot appen anses ha en säkerhetsbrist i stället för en bakdörr. Då blir utvecklaren ombedd att korrigera programmet.

Oönskad programvara på mobila enheter

Denna policy grundar sig i Googles policy om oönskad programvara genom att beskriva principerna för Androids ekosystem och Google Play Butik. Programvara som strider mot dessa principer kan vara skadlig för användarupplevelsen och vi vidtar åtgärder för att skydda användare mot sådan programvara.

Oönskad programvara på mobila enheter

Vi på Google tror att allt annat kommer på köpet om vi väljer att fokusera på användaren. I våra [programvaruprinciper](#) och vår [policy om oönskad programvara](#) finns allmänna rekommendationer för programvara som ger en bra användarupplevelse. Denna policy grundar sig i Googles policy om oönskad programvara genom att beskriva principerna för Androids ekosystem och Google Play Butik. Programvara som strider mot dessa principer kan vara skadlig för användarupplevelsen och vi vidtar åtgärder för att skydda användare mot sådan programvara.

Som vi nämnde i [policyn om oönskad programvara](#) har vi sett att de flesta oönskade programvaror har en eller flera av samma grundläggande egenskaper:

- De är vilseledande och ger ett värdeerbjudande som de inte kan hålla.
- Användaren luras att installera programvaran eller så seriekopplas den på installationen av ett annat program.
- Användaren får inte reda på alla dess grundläggande och viktiga funktioner.
- De påverkar användarens system på oväntade sätt.
- De samlar in eller överför privata uppgifter utan användarnas kännedom.
- De samlar in eller överför privata uppgifter utan säker hantering (t.ex. överföring via HTTPS).
- De ingår i annan programvara utan att nämnas.

På mobila enheter är programvara kodad i form av en app, binärfil, modifieringar av ramverk, osv. För att förhindra programvara som är skadlig för ekosystemet för programvara eller stör användarupplevelsen vidtar vi åtgärder mot kod som bryter mot dessa principer.

Nedan bygger vi vidare på policyn om oönskad programvara i syfte att utöka dess tillämpning till programvara på mobila enheter. Precis som med den tidigare nämnda policyn fortsätter vi att finjustera policyn om oönskad programvara på mobila enheter för att omfatta nya typer av otillåten användning.

Insyn och tydliggörande

All kod ska uppfylla de löften som ges till användaren. Appar ska tillhandahålla alla angivna funktioner. Appar ska inte förvirra användare.

- Appar ska vara tydliga med sina funktioner och mål.
- Förklara uttryckligen och tydligt för användaren vilka systemändringar som görs av appen. Tillåt att användarna granskar och godkänner alla viktiga installationsalternativ och ändringar.
- Programvaran får inte ge en felaktig framställning av statusen på enheten för användare, till exempel genom att hävda att systemet är i ett allvarligt säkerhetsläge eller infekterat med virus.
- Använd inte ogiltig aktivitet som har utformats i syfte att öka annonstrafiken och/eller konverteringarna.
- Vi tillåter inte appar som vilseleder användarna genom att utge sig för att vara någon annan (t.ex. en annan utvecklare, ett annat företag eller ett annat rättssubjekt) eller en annan app. Antyd inte att appen är kopplad till eller auktoriserad av någon som den inte är.

Exempel på överträdelser:

- Annonsbedrägeri
- Identitetsstöld

Skydda användaruppgifter

Var tydlig med hur du kommer åt, använder, samlar in och delar personliga och känsliga användaruppgifter.

Användningen av användaruppgifter måste iakttä alla relevanta policyer om användaruppgifter, om tillämpliga, och vidta alla försiktighetsåtgärder i syfte att skydda sådana uppgifter.

- Ge användarna möjlighet att godkänna insamlingen av data innan du börjar samla in och skicka den från enheten, inklusive data om konton från tredje part, e-post, telefonnummer, installerade appar, filer, plats och andra personliga och känsliga uppgifter som användaren inte förväntar sig samlas in.
- Personliga och känsliga användaruppgifter som samlas in ska hanteras på ett säkert sätt, till exempel genom att överföra dem med moderna krypteringsmetoder (till exempel via HTTPS).
- Programvara, inklusive mobilappar, får bara överföra personliga och känsliga användaruppgifter till servrarna i den mån de är kopplade till appens funktioner.

Exempel på överträdelser:

- Datainsamling (se [Spionprogram](#))
- Otillåten användning av begränsade behörigheter

Exempel på policyer om användaruppgifter:

- [Google Plays policy om användaruppgifter](#)
- [Policy om GMS-krav för användaruppgifter](#)
- [Policy om användaruppgifter i Googles API-tjänst](#)

Skada inte upplevelsen på mobila enheter

Användarupplevelsen ska vara tydlig, lätt att förstå och baseras på tydliga val som fattas av användaren. Den ska tillhandahålla ett tydligt värdeerbjudande och inte störa den marknadsförda eller önskade användarupplevelsen.

- Använd inte annonser som visas för användarna på oväntade sätt, inklusive så att de försämrar eller stör användbarheten av enhetens funktioner, eller visas utanför appens miljö utan att enkelt kunna stängas och utan tillräckligt samtycke och tillräcklig attribution.
- Appar ska inte störa andra appar eller enhetens användbarhet.
- Avinstallationen ska vara tydlig (om tillämpligt).
- Mobil programvara ska inte imitera meddelanden från enhetens operativsystem eller andra appar. Dölj inte varningar till användaren från andra appar eller från operativsystemet, i synnerhet inte sådana som informerar användaren om ändringar i operativsystemet.

Exempel på överträdelser:

- Störande annonser
- Obehörig användning eller imitation av systemfunktioner

Annonsbedrägeri

Annonsbedrägeri är strängt förbjudet. Annonsinteraktioner som genereras i syfte att lura ett annonsnätverk att tro att trafiken kommer från verkligt användarintresse är annonsbedrägeri, vilket är en form av [ogiltig trafik](#). Annonsbedrägeri kan vara en bieffekt av att utvecklare implementerar annonser på otillåtna sätt, t.ex. genom att visa dolda annonser, automatiskt klicka på annonser, ändra eller modifiera information och på annat sätt använda åtgärder som inte utförs av människor (t.ex. spindlar eller botar) eller aktiviteter som utförs av människor och är utformade för att skapa ogiltig annonstrafik. Ogiltig trafik och annonsbedrägeri är skadligt för annonsörer, utvecklare och användare och leder på lång sikt till att förtroendet för ekosystemet av mobilannonser minskar.

Här är några exempel på vanliga överträdelser:

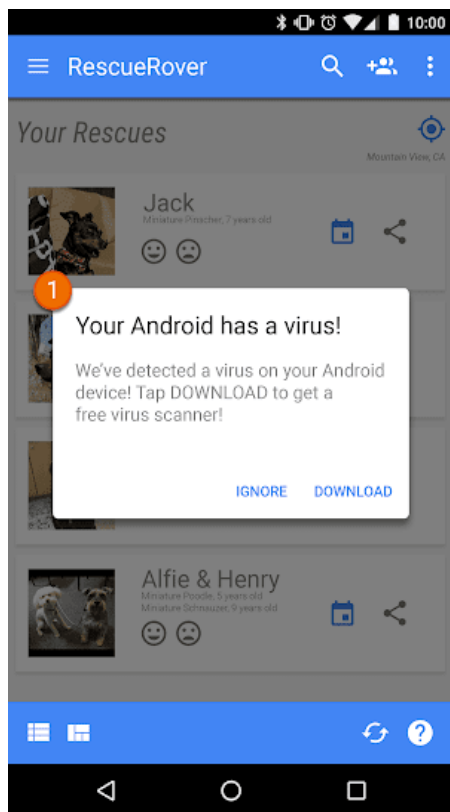
- Appar som renderar annonser som inte är synliga för användaren.
- Appar som automatiskt genererar klick på annonser utan användarens avsikt eller som skapar motsvarande nätverkstrafik i syfte att ge falska klick.
- Appar som skickar falska tillskrivningsklick för installationer i syfte att få betalt för installationer som inte härrör från avsändarens nätverk.
- Appar som visar popup-annonser när användaren inte använder appgränssnittet.
- Appar som förfalskar annonsutrymme, t.ex. appar som kommunicerar till annonsnätverk att de körs på en iOS-enhet när de körs på en Android-enhet, appar som felaktigt framställer vilket paketnamn som genererar intäkter.

Obehörig användning eller imitation av systemfunktioner

Vi tillåter inte appar eller annonser som härmar eller stör systemets funktioner, till exempel aviseringar eller varningar. Aviseringar på systemnivå får bara användas för viktiga funktioner i appen, till exempel en flygbolagsapp som meddelar användarna om specialerbjudanden eller ett spel som meddelar användarna om kampanjer i spelet.

Här är några exempel på vanliga överträdelser:

- Appar eller annonser som levereras via ett systemmeddelande eller en varning:



① Systemmeddelandet som visas i appen används för att visa en annons.

Fler exempel som rör annonser finns i [annonspolicy](#)n.

Identitetsstöld

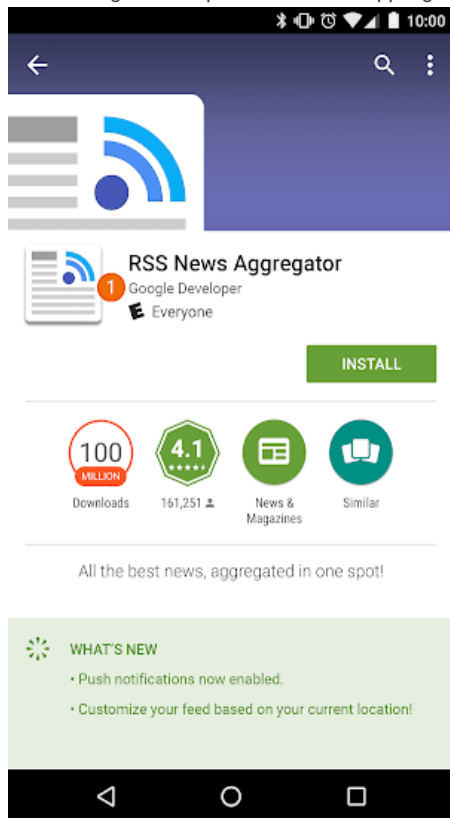
När utvecklare imiterar andra personer eller deras appar vilseleder användare och andra utvecklare skadas. Vi förbjuder appar som vilseleder användare genom att imitera någon annan.

Identitetsstöld

Vi tillåter inte appar som vilseleder användarna genom att utge sig för att vara någon annan (t.ex. en annan utvecklare, ett annat företag eller ett annat rättssubjekt) eller en annan app. Antyd inte att appen är kopplad till eller auktoriserad av någon som den inte är. Var försiktig så att du inte använder appikoner, beskrivningar, titlar eller element i appar som kan vilseleda användarna om appens relation till en annan person eller app.

Här är några exempel på vanliga överträdelser:

- Utvecklare ger falska påståenden om koppling till ett annat företag/en annan utvecklare:



① Det utvecklarnamn som anges för appen antyder en officiell koppling till Google trots att det inte finns någon.

- Apptitlar och appikoner som är så lika titlarna och ikonerna för befintliga produkter eller tjänster att användarna kanske

		Google Maps	Google+	YouTube	Twitter
vilseleds:					
		Google Maps Navigator	Google+ Sharify	YouTube Aggregator	TwitterPro

Intäktsgenerering och annonser

Google Play har stöd för ett flertal vinstgivande strategier för utvecklare och användare, bland annat sponsrad distribution, produkter i appar, prenumerationer och annonsbaserade modeller. Vi kräver att du följer våra policyer för att ge användaren bästa möjliga upplevelse.

Betalningar

Appar som erbjuder köp i butiken eller i appen måste följa följande riktlinjer:

Köp i butiken: Utvecklare som säljer appar och nedladdningar på Google Play måste använda Google Plays betalningssystem.

Köp i appar:

- Utvecklare som säljer åtkomst till spelinnehåll eller produkter i ett spel som laddats ned på Google Play måste använda [fakturerings via Google Play för köp i appar](#) som betalningsmetod.
- Utvecklare som säljer produkter i något annat slags app som laddats ned på Google Play måste använda [fakturerings via Google Play för köp i appar](#) som betalningsmetod utom i följande fall:
 - Betalningen gäller enbart för fysiska produkter
 - Betalningen gäller digitalt innehåll som kan konsumeras utanför själva appen (t.ex. låtar som kan spelas upp i andra musikspelare).
- Virtuella valutor i appar får bara användas i den app eller det spel valutan köptes för.
- Utvecklare får inte ge användarna vilseledande information om apparna eller apparnas tjänster, varor, innehåll och funktioner som de säljer. Om produktbeskrivningen på Google Play hänvisar till funktioner i appen som är avgiftsbelagda eller medför ytterligare avgifter måste det klart framgå i beskrivningen att användarna måste betala för att använda dessa funktioner.
- I appar som innehåller funktioner för att få slumpmässigt utvalda virtuella objekt vid köp (dvs. "lootboxes") måste oddsen för att få sådana objekt tydligt meddelas före köpet.

Här följer några exempel på produkter som stöds för fakturerings via Google Play för köp i appar:

- **Virtuella produkter i spel**, till exempel mynt, juveler, extraliv eller fler omgångar, särskilda föremål eller särskild utrustning, figurer eller avatarer, fler nivåer eller mer speltid.
- **Funktioner eller innehåll i appar**, till exempel den annonsfria versionen av en app eller nya funktioner som inte finns i gratisversionen.
- **Prenumerationstjänster**, till exempel musik, videor och böcker som streamas eller andra medietjänster, digitala publikationer (även tillsammans med en fysisk utgåva) och tjänster för sociala nätverk.
- **Programvara i molnet**, till exempel datalagringstjänster, produktivetsprogramvara för företag och programvara för ekonomihantering.

Här följer några exempel på produkter som för närvarande inte stöds för fakturerings i appar på Google Play:

- **Detaljhandelsvaror**, till exempel matvaror, kläder, husgeråd och elektronik.
- **Serviceavgifter**, till exempel taxi- och transporttjänster, städtjänster, hemkörning av mat, flygresor och biljetter till evenemang.
- **Engångsavgifter för medlemskap eller återkommande betalningar**, till exempel gymkort, bonusprogram eller medlemsprogram som erbjuder tillbehör, kläder eller andra fysiska produkter.
- **Engångsbetalningar**, till exempel överföringar mellan privatpersoner, webbauktioner och donationer.
- **Betalningar av e-fakturer**, till exempel kreditkortsräkningar, räkningar för gas, vatten och el eller kabel- eller telekommunikationstjänster.

Observera att vi erbjuder Google Pay API för appar som säljer fysiska produkter och tjänster. Besök [vår utvecklarsida för Google Pay](#) om du vill veta mer.

Prenumerationer

Du som utvecklare får inte vilseleda användare om de prenumerationstjänster eller det innehåll du erbjuder i appen. Det är avgörande att du är tydlig i kampanjer i appar eller på välkomstskärmar.

I appen: Du måste vara tydlig i dina kampanjerbjudanden. Detta omfattar bland annat utförliga villkor för erbjudandet, kostnaden för prenumerationen, hur lång faktureringsperioden är och om en prenumeration krävs för att använda appen. Användarna ska kunna granska informationen utan att behöva utföra ytterligare åtgärder.

Här är några exempel på vanliga överträdelser:

- Månadsprenumerationer där användarna inte informeras om att debitering och förnyelse av prenumerationen sker varje månad.
- Årsprenumerationer där priset per månad framhävs.
- Priser och villkor för prenumerationer som inte har lokaliserats fullständigt.
- Kampanjer i appar där det inte framgår att användaren får tillgång till innehållet utan en prenumeration (om tillgängligt).

- Missvisande namn på SKU:er för prenumerationer, till exempel Gratis provperiod för en prenumeration som förnyas automatiskt.

Get AnalyzeAPP Premium

16 issues found in your data!
Subscribe to see how we can help

12 months	6 months	1 month
\$9.16/mo Save 35%!	\$12.50/mo Save 11%! MOST POPULAR PLAN	\$14.00/mo

3 Try for \$12.50!

4 Cancele su suscripción en cualquier momento. Por favor, consulte nuestra política de privacidad para más información.

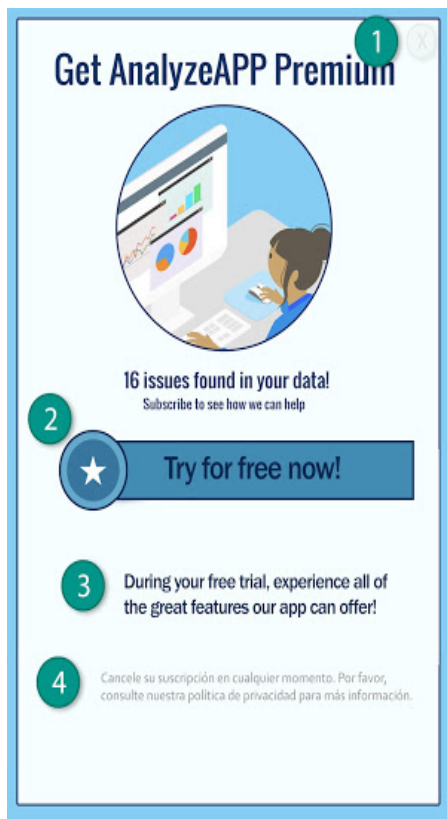
- ① Knappen Stäng syns inte tydligt och det kanske inte framgår för användarna att de får tillgång till funktionerna utan att tacka ja till prenumerationserbjudandet.
- ② Priset för erbjudandet visas bara per månad och det kanske inte framgår för användarna att de debiteras för sex månader i taget när de börjar prenumerera.
- ③ Endast introduktionspriset för erbjudandet visas och det kanske inte framgår för användarna att de debiteras automatiskt när introduktionsperioden löper ut.
- ④ Erbjudandet ska lokaliseras på samma språk som användarvillkoren så att användarna kan göra sig en bild av hela erbjudandet.

Gratis provperioder och introduktionserbjudanden

Innan användare kan registrera sig för prenumerationen: Du måste beskriva villkoren för erbjudandet så tydligt som möjligt, bland annat tidslängden, priset och ange vilket innehåll och vilka tjänster som är tillgängliga. Se till att informera användarna om hur och när en gratis provperiod övergår i en betalprenumeration, hur mycket betalprenumerationen kostar och att användaren kan avsluta prenumerationen om betalversionen inte önskas.

Här är några exempel på vanliga överträdelser:

- Erbjudanden där det inte tydligt meddelas hur länge introduktionspriset eller den gratis provperioden varar.
- Erbjudanden där det inte tydligt meddelas att användaren automatiskt registreras för en betalprenumeration i slutet av erbjudandeperioden.
- Erbjudanden där det inte tydligt framgår att användaren får tillgång till innehållet även utan en provperiod (om tillgängligt).
- Priser och villkor för erbjudanden som inte har lokaliserats fullständigt.



- ① Knappen Stäng syns inte tydligt och det kanske inte framgår för användarna att de får tillgång till funktionerna utan att registrera sig för en gratis provperiod.
- ② I erbjudandet lyfts den gratis provperioden fram och det kanske inte framgår för användarna att de debiteras automatiskt när provperioden löpt ut.
- ③ Det anges inte i erbjudandet hur lång provperioden är och det kanske inte framgår för användarna hur länge de får gratis tillgång till prenumerationens innehåll.
- ④ Erbjudandet ska lokaliseras på samma språk som användarvillkoren så att användarna kan göra sig en bild av hela erbjudandet.

Hantera och säga upp prenumerationer

Utvecklare måste tydligt meddela hur användare kan hantera eller avsluta sin prenumeration på appen.

Det är ditt ansvar att meddela användarna om eventuella ändringar i din prenumerationens-, uppsägnings- eller återbetalningspolicy och att se till att de följer gällande lag.

Annonser

Vi tillåter inte appar som innehåller vilseledande eller störande annonser. Annonser får bara visas i appen som de förekommer i. Vi anser att annonser som visas i din app är en del av appens innehåll. Alla annonser som visas i appen måste därför efterleva våra policyer. Klicka [här](#) om du vill läsa våra policyer gällande annonser för hasardspel.

Använda platsdata för annonser

Appar där användningen av behörighetsbaserad data om enhetens plats har utökats i syfte att visa annonser omfattas av policyn om [personliga och känsliga uppgifter](#). De måste dessutom uppfylla följande krav:

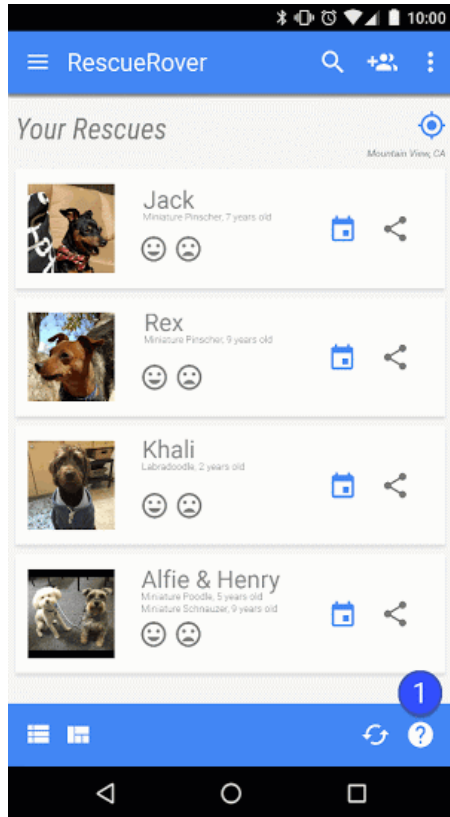
- Det måste vara tydligt för användaren att behörighetsbaserad data om enhetens plats används eller samlas in i annonssyfte. Det måste även dokumenteras i appens obligatoriska sekretesspolicy, bland annat med länkar till relevanta sekretesspolicyer för annonsnätverk som rör användningen av platsdata.
- I enlighet med kraven för [platsbehörighet](#) får platsbehörighet endast begäras för implementering av befintliga funktioner eller tjänster i appen. Du får inte begära platsbehörighet för enheten om annonsvisning är det enda syftet.

Vilseledande annonser

Annonser får inte efterlikna eller imitera användargränssnittet i en app eller systemmeddelanden eller varningar i ett operativsystem. Det måste vara tydligt för användaren vilken app som visar varje annons.

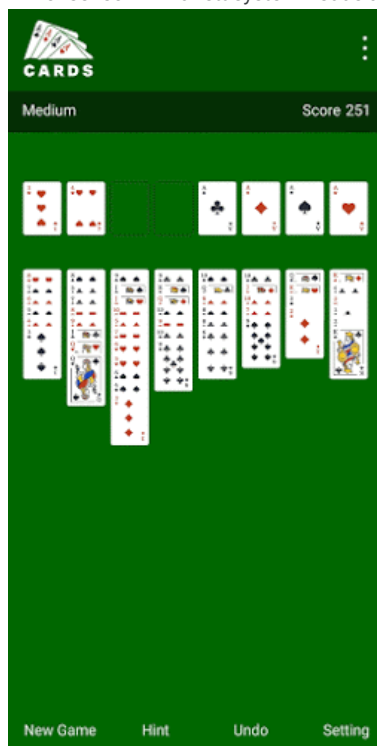
Här är några exempel på vanliga överträdelser:

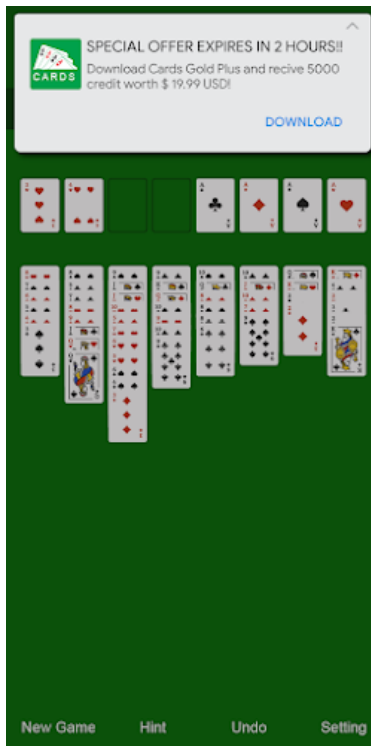
- Annonser som liknar gränssnittet i en app:



① Frågetecknet i den här appen är en annons som leder till en extern målsida.

- Annonser som liknar ett systemmeddelande:





Exemplen ovan visar annonser som liknar olika systemmeddelanden.

Intäktsgenerering via låsskärm

Appar får inte införa annonser eller funktioner som genererar intäkter på enheters låsskärmar, såvida inte appens enda syfte är att fungera som låsskärm.

Störande annonser

Störande annonser är annonser som visas för användarna på oväntade sätt, vilket kan leda till oavsiktliga klick eller till att enhetsfunktionernas användbarhet försämras eller störs.

Appen får inte tvinga användare att klicka på annonser eller uppge personuppgifter i annonseringssyfte innan de kan använda appen till fullo. Mellansidesannonser får bara visas i appen som de tillhör. Om mellansidesannonser eller andra annonser som stör normal användning av appen visas måste de gå att stänga utan negativa konsekvenser.

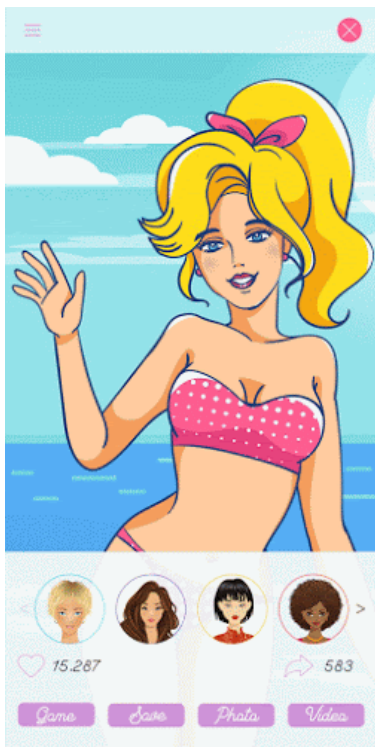
Här är några exempel på vanliga överträdelser:

- Annonser som tar upp hela skärmen eller stör normal användning, och som inte har något tydligt sätt att stänga annonsen:

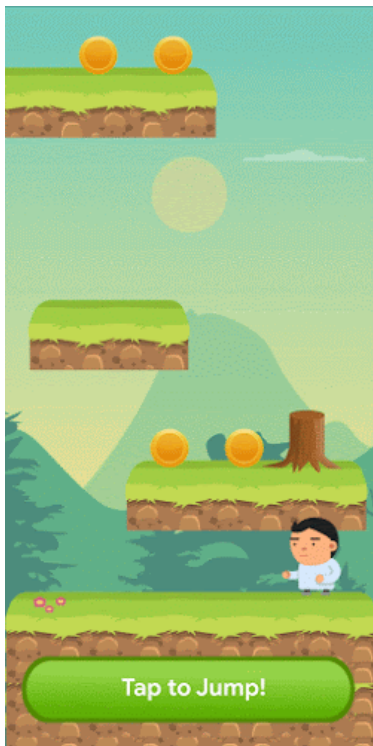


① Det finns ingen stängningsknapp för den här annonsen.

- Annonser som tvingar användaren att klicka på dem genom att använda en falsk stängningsknapp, eller genom att annonserna plötsligt visas i delar av appen där användaren oftast trycker på en annan funktion.



En annons med en falsk stängningsknapp.



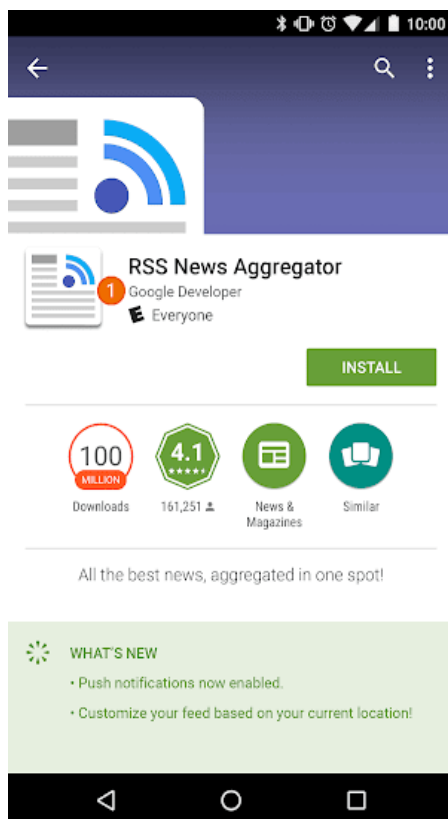
En annons som plötsligt visas i ett område där användaren är van vid att trycka på funktioner i appen.

Störa appar, tredjepartsannonser eller enhetsfunktioner

Annonser som är kopplade till din app får inte störa andra appar, annonser eller enhetens funktion, inklusive system- eller enhetsknappar och -portar. Detta omfattar överlagringar, tillhörande funktioner och annonsenheter i form av widgetar. Annonser får bara visas i appen som de förekommer i.

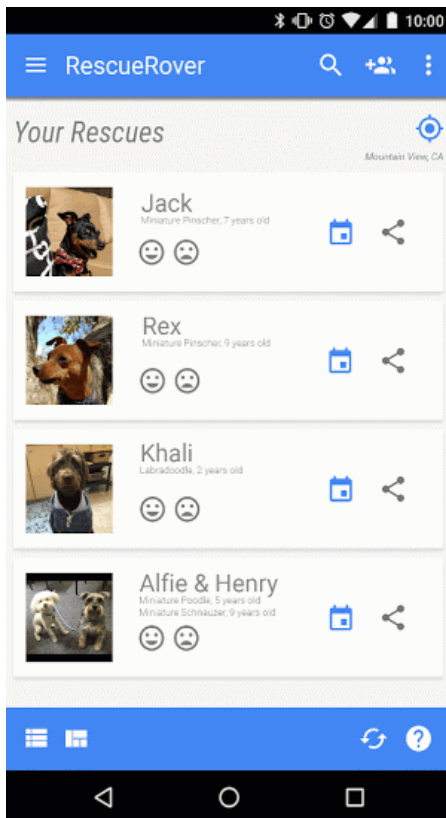
Här är några exempel på vanliga överträdelser:

- Annonser som visas utanför appen som de tillhör:



Beskrivning: Användaren navigerar till startskärmen från appen. Plötsligt visas en annons på startskärmen.

- Annonser som startas av knappen Start sida eller andra funktioner som uttryckligen är avsedda att avsluta appen:

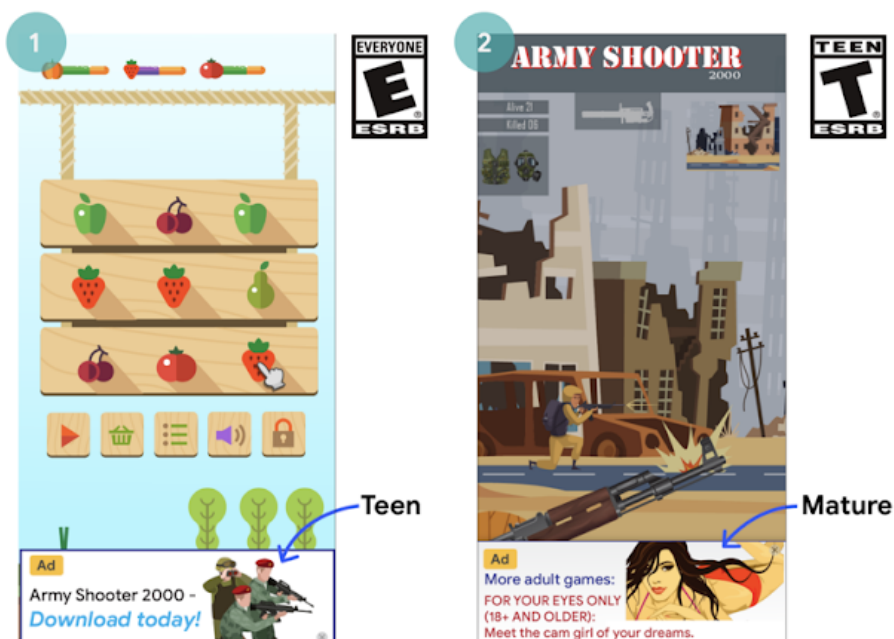


Beskrivning: Användaren försöker avsluta appen och navigera till startskärmen, men i stället avbryts det förväntade flödet av en annons.

Olämpliga annonser

Annonserna som visas i appen måste vara lämpliga för appens målgrupp, även om innehållet i sig följer våra policyer.

Här är ett exempel på en vanlig överträdelse:



- ① Den här annonsen är olämplig (Tonåring) för appens avsedda målgrupp (Från 7 år)
- ② Den här annonsen är olämplig (Vuxen) för appens avsedda målgrupp (Från 12 år)

Användning av Androids reklam-id

I version 4.0 av Google Play-tjänsterna introducerades nya API:er och ett id som kan användas av annonserings- och analysleverantörer. Villkoren för användning av detta id följer nedan.

- **Användning:** Androids reklam-id får endast användas för annonsering och användningsanalys. Vid varje åtkomst till detta id måste inställningen Välj bort intressebaserad annonsering eller Välj bort Anpassning av annonser kontrolleras.
- **Koppling till uppgifter som kan kopplas till en specifik individ och andra identifierare**
 - Användning för annonsering: Detta reklam-id får inte kopplas till beständiga enhetsidentifierare (till exempel SSAID, MAC-adresser, IMEI-kod osv.) i något annonseringssyfte. Ett reklam-id får endast kopplas till uppgifter som kan kopplas till en specifik individ efter användarens uttryckliga samtycke.
 - Användning för analyser: Ett reklam-id får endast kopplas till uppgifter som kan kopplas till en specifik individ eller beständiga enhetsidentifierare (till exempel SSAID, MAC-adress, IMEI-kod osv.) efter användarens uttryckliga samtycke.
- **Respektera användarnas val.** Vid återställning till ett nytt reklam-id får detta inte kopplas till ett tidigare reklam-id eller till data som härrör från ett tidigare reklam-id utan användarens uttryckliga samtycke. Du måste också rätta dig efter det val som användaren har gjort för inställningen Välj bort intressebaserad annonsering eller Välj bort Anpassning av annonser. Om användaren har aktiverat denna inställning får du inte använda detta reklam-id för att skapa användarprofiler för annonseringsändamål eller för att rikta in användare med anpassad annonsering. Till de aktiviteter som är tillåtna hör innehållsbaserad annonsering, frekvenstak, konverteringssparning, rapportering och säkerhet och bedrägeriupptäckt.
- **Insyn för användarna.** Användarna måste upplysas om att detta reklam-id används och samlas in och att de här villkoren efterlevs i ett juridiskt adekvat sekretessmeddelande. Läs mer om våra sekretessstandarder i vår policy om [användaruppgifter](#).
- **Följ användarvillkoren.** Detta reklam-id får endast användas i enlighet med dessa villkor. Det gäller även för eventuella parter som du delar det med i ditt företag. Alla appar som laddas upp och publiceras på Google Play måste innehålla detta reklam-id (om det finns tillgängligt på enheten) i stället för andra enhets-id:n för alla annonseringsändamål.

Programmet för familjeannonser

Om du visar annonser i appen och endast barn ingår i målgruppen i enlighet med [familjepolicyn](#) måste du använda ett annons-SDK som har självcertifierat att det efterlever Google Plays policyer, inklusive certifieringskraven för annons-SDK:er nedan. Om både barn och äldre användare ingår i målgruppen för appen måste du implementera metoder för ålderskontroll och säkerställa att alla annonser som visas för barn kommer från ett av dessa självcertifierade annons-SDK:er. Endast självcertifierade annons-SDK:er får användas i appar som ingår i programmet Avsett för familjer.

Du måste bara använda Google Play-certifierade annons-SDK:er om du visar annonser för barn via annons-SDK:er. Följande är tillåtet om annons-SDK:et inte är självcertifierat för Google Play, men tänk på att du bär ansvaret för att säkerställa att annonsinnehåll och metoder för datainsamling efterlever Plays [policy om användaruppgifter](#) och [familjepolicy](#):

- Intern annonsering där SDK:er används för hantering av korsmarknadsföreläggning av dina appar eller annan media och andra produkter du säljer.
- Ingå direktavtal med annonsörer där SDK:er används för hantering av annonsutrymme.

Krav för certifiering av annons-SDK

- Definiera vad som utgör olämpligt innehåll och beteende i annonser och förbjud det i villkoren eller policyn för annons-SDK:et. Definitionerna ska följa Plays programpolicy för utvecklare.
- Utveckla en metod för att klassificera annonsmaterial efter lämplig åldersgrupp. Dessa åldersgrupper måste åtminstone inkludera Ingen åldersgräns och Olämpligt för barn. Klassificeringsmetoden måste överensstämma med den metod som Google tillhandahåller för SDK:er som har fyllt i intresseanmälan nedan.
- Tillåt att utvecklare begär, per app eller per begäran, att appen behandlas som avsedd för barn gällande visning av annonser. Sådan behandling måste efterleva alla tillämpliga lagar och föreskrifter, till exempel [den amerikanska lagen om barns personuppgifter på webben \(COPPA\)](#) och EU:s [allmänna dataskyddsförordning \(GDPR\)](#). Google Play kräver också att annons-SDK:er inaktiverar anpassade annonser, intressebaserad annonsering och remarketing när appen behandlas som avsedd för barn.
- Tillåt att utgivare väljer annonsformat som följer [Plays policy om familjeannonser och intäktsgenerering](#) och uppfyller kraven i [programmet Godkänd av lärare](#).
- Se till att allt annonsmaterial som används i annonsering för barn som säljs via budgivning i realtid har granskats och att budgivarna är medvetna om de särskilda integritetskraven.

- Tillhandahåll tillräckligt underlag, till exempel de uppgifter som anges i [intresseanmälan](#) nedan, för att Google ska kunna verifiera att annons-SDK:et efterlever alla certifieringskrav och svara inom rimlig tid på eventuella efterföljande förfrågningar om information.

Obs! Annon-SDK:er måste ha stöd för visning av annonser som efterlever alla relevanta bestämmelser och förordningar gällande barn som kan tillämpas på deras utgivare.

Förmedlingskrav för annonsvisningsplattformar gällande annonser som visas för barn:

- Använd endast Play-certifierade annons-SDK:er eller implementera de skyddsåtgärder som krävs för att säkerställa att alla annonser som visas via medling efterlever dessa krav.
- Förmedla nödvändig information till plattformar för medling om annonsinnehållets klassificering och eventuell tillämplig behandling som avsedd för barn.

Här hittar utvecklare en [lista över självcertifierade annons-SDK:er](#).

Utvecklare kan även dela detta [formulär för intresseanmälan](#) med annons-SDK:er som vill självcertifieras.

Butiksuppgifter och marknadsföring

Din apps marknadsföring och synlighet påverkar betydligt butikens kvalitet. Undvik butiksuppgifter med skräp, marknadsföring av låg kvalitet och att på ett oärligt sätt förbättra en apps synlighet på Google Play.

Marknadsföring av appar

Vi tillåter inte appar som direkt eller indirekt utnyttjar marknadsföringsmetoder som är vilseledande eller skadliga för användare eller utvecklare. Detta omfattar appar där följande förekommer:

- Användning av vilseledande annonser på webbplatser, i appar eller andra egendomar, till exempel aviseringar som liknar systemmeddelanden och varningar.
- Marknadsföring eller installationsstrategier som omdirigerar användare till Google Play eller laddar ned appar utan att användaren kan göra ett välinformerat val om det.
- Önskad marknadsföring via sms-tjänster.

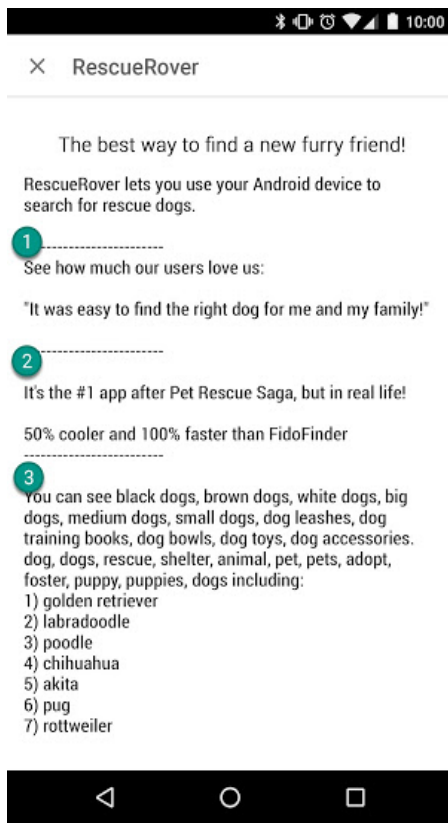
Det är ditt ansvar att se till att eventuella annonsnätverk eller närstående bolag som är kopplade till din app också följer dessa policyer och inte använder några otillåtna marknadsföringsmetoder.

Metadata

Vi tillåter inte appar med vilseledande, felaktigt formaterad, otydlig, irrelevant, överflödigt eller olämplig metadata. Det gäller bland annat appbeskrivningen, utvecklarens namn, appens namn, ikon, skärmdumpar och kampanjbilder. Utvecklare måste ge en tydlig och välskriven beskrivning av appen. Det är heller inte tillåtet att använda anonyma användarrekommendationer i appens beskrivning.

Utöver de krav som anges här kan du behöva ange ytterligare information om metadata i enlighet med Plays specifika utveckelpolicy.

Här är några exempel på vanliga överträdelser:



- ① Anonyma användarrekommandationer
- ② Jämförelser av uppgifter mellan appar och varumärken
- ③ Väggar av text eller horisontala eller vertikala listor av ord

Här är några exempel på olämpliga texter, bilder eller videor i uppgifterna:

- Bilder eller videor med sexuellt innehåll. Undvik bilder och videor som innehåller bröst, rumpor, genitalier eller andra kroppsdelar eller annat innehåll som ofta sexualiseras. Detta gäller både tecknat och otecknat material.
- Användning av svordomar, vulgärt språk eller annat språk som är olämpligt för en allmän målgrupp i appens butiksuppgifter.
- Framträdande våldsskildringar på appikoner, i kampanjbilder eller i videor.
- Skildringar av illegal användning av droger. Innehåll i butiksuppgifterna måste vara lämpligt för alla målgrupper, även om det syftar till att vara utbildande, dokumentärt, vetenskapligt eller konstnärligt.

Här är några bra metoder:

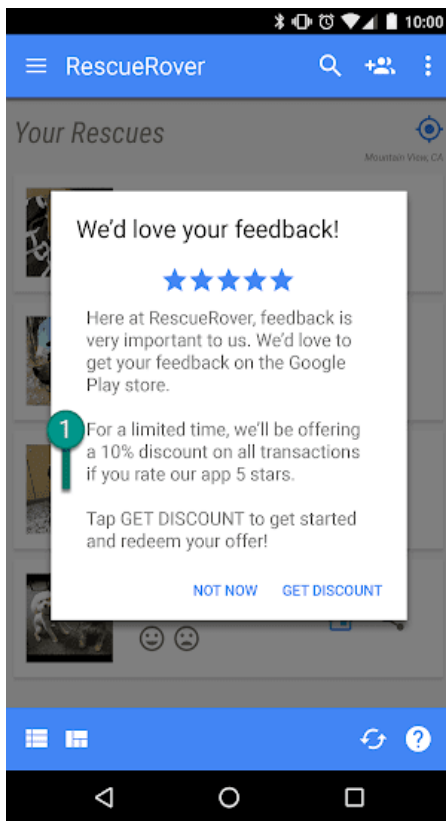
- Betona vad som är bra med din app. Dela intressanta och spännande fakta så att användarna förstår vad som gör appen speciell.
- Försäkra dig om att appens titel och beskrivning beskriver appens funktioner på ett korrekt sätt.
- Undvik upprepade eller irrelevanta sökord eller hänvisningar.
- Skriv en kortfattad och saklig beskrivning för appen. Kortare beskrivningar fungerar bättre, särskilt på enheter med små skärmar. Beskrivningar som är överdrivet långa, detaljerade, felaktigt formaterade eller repetitiva kan utgöra en överträdelse av policyn.
- Tänk på att uppgifterna ska vara lämpliga för en allmän målgrupp. Använd inte text, bilder eller videor som är olämpliga i butiksuppgifterna och följ riktlinjerna ovan.

Användarbetyg, recensioner och installationer

Utvecklare får inte försöka ändra placeringen för appar i Google Play. Detta omfattar, men är inte begränsat till, att höja produktbetyg, recensioner eller antal installationer på otillåtna sätt, såsom bedrägliga installationer och att erbjuda ersättning för recensioner, betyg och installationer.

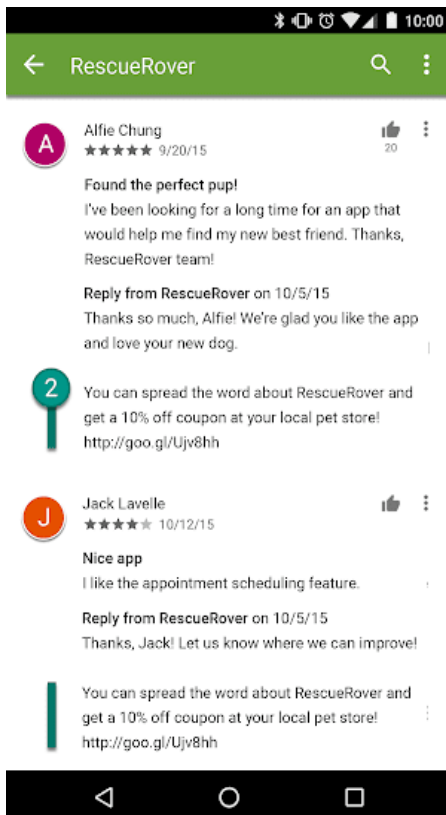
Här är några exempel på vanliga överträdelser:

- Be användarna att betygsätta din app och erbjuda ersättning:



① Det här meddelandet erbjuder användarna en rabatt i utbyte mot ett högt betyg.

- Skicka betyg flera gånger för att påverka appens placering på Google Play.
- Skicka eller uppmuntra användare att skicka recensioner som innehåller olämpligt innehåll, inklusive partners, kuponger, spelkoder, e-postadresser eller länkar till webbplatser eller andra appar:



② Den här recensionen uppmuntrar användare att marknadsföra appen RescueRover genom att erbjuda en kupong.

Betyg och recensioner är riktmärken för appens kvalitet. Användarna är beroende av att de är äkta och relevanta. Här är några bra tips när du svarar på användarrecensioner:

- Fokusera på problemen i användarens kommentarer när du svarar och fråga inte efter ett högre betyg.
- Ta med referenser till praktiska resurser som en supportadress eller en sida med vanliga frågor och svar.

Innehållsrankningar

Innehållsklassificeringar på Google Play tillhandahålls av IARC (International Age Rating Coalition) och är utformade för att hjälpa utvecklare att förse användarna med lokalt relevanta innehållsklassificeringar. Lokala klassificeringsorgan har riktlinjer som används för att avgöra den nivå av mognad som krävs för innehållet i en app. Vi tillåter inte appar utan innehållsklassificering på Google Play.

Så här används innehållsklassificeringar

Innehållsklassificeringar är avsedda att informera kunder, i synnerhet föräldrar, om innehåll i appar som kan vara stötande. De bidrar även till att blockera eller filtrera innehållet i vissa områden eller till vissa användare där så krävs enligt lag. Dessutom används de för att avgöra om appen uppfyller villkoren för vissa utvecklarprogram.

Så här tilldelas innehållsklassificeringar

För att få en innehållsklassificering måste du fylla i ett [klassificeringsformulär i Play Console](#) som handlar om apparnas innehåll. Din app tilldelas en innehållsklassificering från flera klassificeringsorganisationer baserat på svaren i frågeformuläret. Missledande information om appens innehåll kan resultera i att den tas bort eller stängs av tillfälligt. Det är därför viktigt att du ger korrekta svar i frågeformuläret.

För att undvika att appen listas som Ingen klassificering måste du fylla i klassificeringsformuläret för varje ny app som skickas till Play Console, samt för alla befintliga appar som är aktiva på Google Play.

Om du gör ändringar i appens innehåll eller funktioner som påverkar svaren i klassificeringsformuläret måste du skicka in ett nytt formulär i Play Console.

Besök [hjälpcentret](#) om du vill veta mer om de olika [klassificeringsorganisationerna](#) och om hur du fyller i klassificeringsformuläret.

Överklaga klassificeringar

Om du anser att IARC har gett din app en felaktig innehållsklassificering har du rätt att överklaga direkt till IARC med hjälp av länken som anges i certifikatmeddelandet.

Nyheter

Appar som väljer kategorin Nyheter men uppvisar innehåll som inte uppfyller dessa krav tillåts inte i kategorin Nyheter i Play Butik. Nyhetsappar som kräver att en användare köper ett medlemskap måste ge användarna en förhandsgranskning av innehållet innan de köper.

Nyhetsappar **MÅSTE**

- tillhandahålla tillräcklig information om nyhetsutgivaren och medverkande, inklusive ett tydligt angivet ägarskap
- ha en webbplats eller en sida i en app med giltiga kontaktuppgifter till nyhetsutgivaren.

Nyhetsappar **FÅR INTE**

- innehålla markanta stavfel och grammatiska fel
- endast innehålla statiskt innehåll
- ha affiliate-marknadsföring eller annonsintäkter som primärt syfte.

Appar med sammanställda nyheter måste tydligt ange innehållets publiceringskälla i appen och alla källor måste uppfylla kraven i nyhetspolicyn.

Spam och minimikrav på funktion

Appar måste uppfylla grundläggande krav på funktion med hänsyn till användarnas upplevelse. Appar som kraschar, på andra sätt inte uppfyller kraven för en fungerande användarupplevelse eller vars enda syfte är att spamma användare eller Google Play är inte appar som utökar katalogen på ett meningsfullt sätt.

Spam

Vi tillåter inte appar som visar spam för användarna eller på Google Play, exempelvis appar varifrån oönskade meddelanden skickas till användarna, eller appar som är repetitiva och av låg kvalitet.

Spammeddelanden

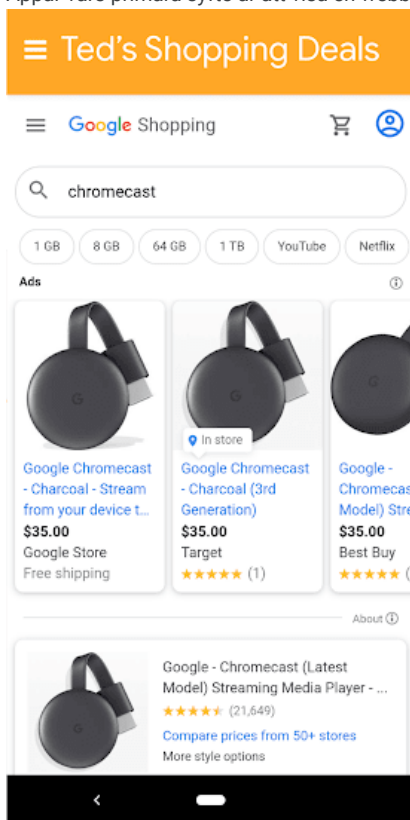
Vi tillåter inte appar som skickar sms, e-post eller andra meddelanden för användarens räkning utan att användaren kan bekräfta innehållet eller de avsedda mottagarna.

WebViews- och affiliate-spam

Vi tillåter inte appar vars primära syfte är att driva affiliate-trafik till en webbplats eller att visa en webbplats utan tillåtelse från webbplatsens ägare eller administratör.

Här är några exempel på vanliga överträdelser:

- En app vars primära syfte är att mot ersättning driva trafik till en webbplats så att användare registrerar sig eller köper något där.
- Appar vars primära syfte är att visa en webbplats utan tillåtelse:



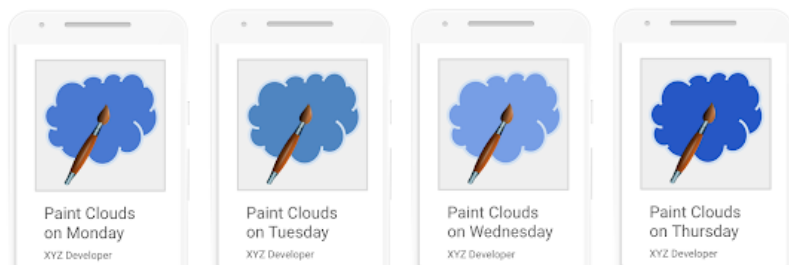
Denna app heter Ted's Shopping Deals och den tillhandahåller endast en WebView av Google Shopping.

Repetitivt innehåll

Vi tillåter inte appar som endast tillhandahåller samma upplevelser som andra appar som redan finns på Google Play. Appar bör ge användarna mervärde genom att tillhandahålla innehåll eller tjänster som är unika.

Här är några exempel på vanliga överträdelser:

- Kopiera innehåll från andra appar utan att lägga till originellt innehåll eller värde.
- Skapa flera appar med snarlika funktioner, innehåll och användarupplevelser. Om det finns väldigt lite innehåll i apparna bör utvecklaren överväga att sammanställa innehållet i en enda app.



Visa annonser

Vi tillåter inte appar vars primära syfte är att visa annonser.

Här är några exempel på vanliga överträdelser:

- Appar där mellansidesannonser visas efter varje åtgärd användaren vidtar, vilket inbegriper men är inte begränsat till klick, svepningar osv.

Minimikrav på funktion

Säkerställ att användarupplevelsen i appen är stabil, engagerande och följsam.

Här är några exempel på vanliga överträdelser:

- Appar som inte har utformats för att göra något eller fylla någon funktion.

Defekt funktion.

Vi tillåter inte appar som kraschar, tvingas att stängas, låser sig eller på andra sätt inte fungerar som de ska.

Här är några exempel på vanliga överträdelser:

- Appar som **inte** går att installera.
- Appar som går att installera men **inte** att läsa in.
- Appar som går att läsa in men som **inte** svarar.

Andra program

Appar som är utformade för andra Android-upplevelser och som distribueras via Google Play kan omfattas av programspecifika policykrav utöver de innehållspolicyer som anges på andra platser i detta policycenter. Granska nedanstående lista och ta reda på om någon av dessa policyer gäller din app.

Android Instant Apps

Vårt mål med Android Instant Apps är att skapa behagliga och smidiga användarupplevelser samtidigt som vi iakttar högsta standard för sekretess och säkerhet. Våra policyer är utformade i syfte att stödja det målet.

Utvecklare som väljer att distribuera Android Instant Apps via Google Play måste följa följande policyer, utöver övriga [programpolicyer för utvecklare på Google Play](#).

Identitet

Utvecklare måste integrera [Smart Lock för lösenord](#) för snabbappar med inloggningsfunktioner.

Stöd för länkar

Utvecklare av Android Instant Apps måste stödja länkar för andra appar. Om utvecklarens snabbapp eller installerade app innehåller länkar som kan omvandlas till en snabbapp måste utvecklaren hänvisa användare till den snabbappen i stället för att exempelvis läsa in länkarna i [WebView](#).

Tekniska specifikationer

Utvecklare måste följa de tekniska specifikationer och krav för Android Instant Apps som anges av Google och som kan ändras emellanåt. Detta inkluderar de specifikationer och krav som anges i [vår offentliga dokumentation](#).

Erbjuda appinstallation

Snabbappen får erbjuda användaren den installerbara versionen, men det får inte vara snabbappens huvudsakliga syfte. Om installation erbjuds måste utvecklare:

- Använda [ikonen Ladda ned app från Material Design](#) och etiketten Installera som installationsknapp.
- Inte ha fler än 2–3 implicita installationsuppsmaningar i snabbappen.
- Inte presentera installationsuppsmaningen för användarna med hjälp av en banner eller annan annonsliknande teknik.

Du hittar mer information om snabbappar och riktlinjer för användarupplevelser i [Bästa metoder för användarupplevelse](#).

Ändra enhetens status

Snabbappar får inte genomföra ändringar av användarens enhet som varar längre än sessionen för snabbappen. Snabbappar får till exempel inte ändra användarens bakgrund eller skapa en widget på startskärmen.

Appens synlighet

Utvecklare måste se till att snabbappar är synliga för användare på ett sådant sätt att användaren alltid är medveten om att snabbappen körs på enheten.

Enhetsidentifierare

Snabbappar får inte ha åtkomst till enhetsidentifierare som både (1) finns kvar efter det att snabbappen har slutat att köras (2) inte kan återställas av användaren. Exempelen omfattar men är inte begränsade till

- Build Serial
- Mac-adresser till eventuella nätverkskretsar
- IMEI, IMSI

Snabbappar får ha åtkomst till telefonnummer om dessa har samlats in med körningsbehörighet. Utvecklaren får inte försöka skapa ett fingeravtryck för användare med hjälp av dessa identifierare eller andra metoder.

Nätverkstrafik

Nätverkstrafik inifrån snabbappen måste krypteras med ett TLS-protokoll, till exempel HTTPS.

Familjer

Google Play erbjuder en bred plattform för utvecklare där de kan visa upp innehåll av hög kvalitet som är lämpligt för alla åldrar och passar hela familjen. Du ansvarar för att säkerställa att din app lämpar sig för barn och efterlever all relevant lagstiftning innan du skickar en app till programmet Avsett för familjer eller skickar en app som riktar sig till barn till Google Play Butik.

Läs mer om arbetsgången för familjeappar och gå igenom den interaktiva checklistan på Academy for App Success.

Utforma appar för barn och familjer

Teknik används i allt större utsträckning för att berika familjens vardag och föräldrar efterfrågar säkert innehåll av hög kvalitet som de kan dela med sina barn. Din app kanske särskilt riktar sig till barn, eller så dras barn till din app ändå. Google Play vill underlätta för dig att säkerställa att din app är säker för alla användare, även familjer.

Ordet "barn" har olika betydelse på olika platser och i olika sammanhang. Det är viktigt att du rådgör med ditt juridiska ombud för att klargöra vilka förbindelser och/eller åldersgränser som gäller för din app. Eftersom du är expert på hur din app fungerar räknar vi med din hjälp för att se till att appar på Google Play är säkra att använda för familjer.

Appar som särskilt riktar sig till barn måste delta i programmet Avsett för familjer. Du kan delta i programmet Avsett för familjer även om appen riktar sig till både barn och äldre målgrupper. Alla appar som deltar i programmet Avsett för familjer kan klassificeras för [programmet Godkänd av lärare](#), men vi kan inte garantera att appen inkluderas i programmet. Om du väljer att inte delta i programmet Avsett för familjer måste du ändå efterleva kraven i familjepolicyn för Google Play nedan och samtliga [programpolicyer för utvecklare på Google Play](#) och [distributionsavtalet för utvecklare](#).

Krav för Play Console

[Målgrupp och innehåll](#)

I avsnittet **Målgrupp och innehåll** i Google Play Console måste du ange målgruppen för appen innan publiceringen genom att välja åldersgrupper på listan som visas. Oavsett vad du anger i Google Play Console kan bedömningen av den uppgivna åldersgruppen påverkas av eventuella bilder och termer i appen som kan anses vara riktade till barn. Google Play förbehåller sig rätten att utföra en egen granskning av informationen du tillhandahåller om appen och avgöra huruvida den angivna målgruppen är korrekt.

Om du väljer en målgrupp där endast vuxna ingår men Google bedömer att den inte stämmer eftersom appen riktar sig till både barn och vuxna får du möjlighet att klargöra för användarna att appen inte riktar sig till barn genom att märka den med en varning.

Du bör endast välja flera åldersgrupper som målgrupp om appen är avsedd för användare i de valda åldersgrupperna och du har säkerställt appens lämplighet. Om appen till exempel är avsedd för småbarn och barn i förskoleåldern väljer du bara Upp till 5 år som åldersgrupp för appen. Om appen riktar sig till en specifik årskurs väljer du den åldersgrupp som bäst stämmer överens med årskursen. Välj bara åldersgrupper där både barn och vuxna ingår om appen verkligen riktar sig till alla åldrar.

Uppdateringar av avsnittet Målgrupp och innehåll

Du kan när som helst uppdatera informationen om appen i avsnittet Målgrupp och innehåll i Google Play Console. Informationen visas i Google Play Butik först efter en [appuppdatering](#). Ändringar i det här avsnittet i Google Play Console kan dock granskas för policyefterlevnad innan appuppdateringen skickas in.

Vi rekommenderar att du meddelar befintliga användare om du ändrar åldersgruppen för appen, börjar att visa annonser eller erbjuda köp i appen. Detta görs antingen i avsnittet Nyheter på sidan med butiksuppgifter för appen eller via aviseringar i appen.

Felaktig framställning i Play Console

Felaktig framställning av någon information om appen i Play Console, inbegripet i avsnittet Målgrupp och innehåll, kan resultera i att appen tas bort eller stängs av. Därför är det viktigt att uppgifterna är korrekta.

Krav för familjepolicyn

Följande krav måste efterlevas om barn ingår i en av målgrupperna för appen. Om kraven inte efterlevs kan det resultera i att appen tas bort eller stängs av.

1. **Appens innehåll:** Innehåll i appen som är tillgängligt för barn måste vara lämpligt för dem.
2. **Svar i Google Play Console:** Du måste uppgge korrekta svar på frågor om appen i Google Play Console och uppdatera svaren så att de överensstämmer med eventuella ändringar av appen.
3. **Annonser:** Om annonser visas för barn eller användare i okänd ålder i appen måste du göra följande:
 - Endast visa annonser från [Google Play-certifierade annons-SDK:er](#) för sådana användare.
 - Säkerställa att annonser som visas för sådana användare inte innehåller intressebaserad annonsering (annonsering som är inriktad på enskilda användare med vissa egenskaper baserat på hur de använder internet) eller remarketing (annonsering som är inriktad på enskilda användare baserat på tidigare interaktioner med en app eller webbplats).
 - Säkerställa att annonser som visas för sådana användare är lämpliga för barn.
 - Säkerställa att annonser som visas för sådana användare uppfyller annonsformatkraven för Familjer.
 - Säkerställa att all tillämplig lagstiftning och alla branschstandarder för annonsering som riktar sig till barn efterlevs.
4. **Insamling av data:** Du måste meddela om några [personliga och känsliga uppgifter](#) samlas in från barn i appen, även via API:er och SDK:er som används eller anropas i appen. Känsliga uppgifter från barn omfattar men är inte begränsat till autentiseringsuppgifter, sensordata från mikrofoner och kameror, enhetsdata, Android-id, annonsanvändning och annons-id.
5. **API:er och SDK:er:** Du måste säkerställa att eventuella API:er och SDK:er implementeras korrekt i appen.
 - Appar som endast riktar sig till barn får inte innehålla några API:er eller SDK:er som inte är godkända för tjänster som riktar sig till barn. Detta omfattar Inloggning med Google (och alla andra Google API-tjänster som har åtkomst till data från ett Google-konto), Google Plays speltjänster och alla andra API-tjänster från Google som använder OAuth-teknik för autentisering och auktorisering.
 - Implementera inte API:er och SDK:er som inte är godkända för tjänster som riktar sig till barn i appar som riktar sig både till barn och äldre målgrupper om de inte skyddas av en [skärm för ålderskontroll](#) eller implementeras på sådant vis att uppgifter om barn inte samlas in (t.ex. tillhandahålla Inloggning med Google som valfri funktion). Appar som riktar sig till både barn och äldre målgrupper får inte kräva att användarna loggar in eller använder appinnehåll via API:er eller SDK:er som inte är godkända för tjänster som riktar sig till barn.
6. **Sekretesspolicy:** Du måste ange en länk till sekretesspolicyn på sidan med butiksuppgifter för appen. Länken måste alltid vara tillgänglig så länge som appen finns i Play Butik och den måste leda till en sekretesspolicy som bland annat innehåller en korrekt beskrivning av insamlingen och användningen av data i appen.
7. **Särskilda begränsningar:**

- Om förstärkt verklighet (AR) används i appen måste du inkludera en säkerhetsvarning som visas direkt när AR-avsnittet startas. Varningen ska innehålla följande:
 - Ett lämpligt meddelande om vikten av föräldrakontroll.
 - En påminnelse om vikten av att vara medveten om de fysiska risker som den verkliga världen medför (till exempel: Var uppmärksam på omgivningen).
- Användning av enheter som inte är lämpliga för barn (t.ex. Daydream och Oculus) får inte krävas för appen.

8. **Juridisk efterlevnad:** Du måste säkerställa att appen, inbegripet alla API:er eller SDK:er som används i eller anropas av appen, efterlever den amerikanska lagen [COPPA \(Children's Online Privacy and Protection Act\)](#), [EU:s allmänna dataskyddsförordning \(GDPR\)](#) och alla andra tillämpliga lagar och bestämmelser.

Här är några exempel på vanliga överträdelser:

- Appar som marknadsförs som barnspel i butiksuppgifterna men innehållet är endast lämpligt för vuxna.
- Appar där API:er vars användarvillkor förbjuder användning i appar som riktar sig till barn har implementerats.
- Appar där alkohol, tobak eller begränsade ämnen beskrivs på ett förskönande sätt.
- Appar som innehåller verkligt eller simulerat hasardspel.
- Appar som innehåller våld, blodsutgjutelse eller stötande innehåll är inte lämpliga för barn.
- Appar där dejtingtjänster eller sex- eller äktenskapsrådgivning erbjuds.
- Appar som innehåller länkar till webbplatser vars innehåll som strider mot Google Plays [programpolicy för utvecklare](#).
- Appar som visar barnförbjudna annonser (t.ex. våldsamt innehåll, sexuellt innehåll, hasardspelsinnehåll) för barn. Du kan läsa mer om Google Plays policyer om annonsering, köp i appar och kommersiellt innehåll för barn i [policyerna om familjeannonser och intäktsgenerering](#).

Programmet Avsett för familjer

Appar som särskilt riktar sig till barn måste delta i programmet Avsett för familjer. Om appen riktar sig till alla, även barn och familjer, kan du ansöka om att delta i programmet.

Innan du kan få tillgång till programmet måste din app uppfylla alla krav i familjepolicyn och behörighetskraven för Avsett för familjer, utöver de krav som beskrivs i [Google Plays programpolicy för utvecklare](#) och [distributionsavtalet för utvecklare](#).

Du hittar mer information om hur du ansöker om att din app ska ingå i programmet genom att klicka [här](#).

Behörighet till programmet

Både annons- och appinnehållet i alla appar som ingår i programmet Avsett för familjer måste vara relevant och lämpligt för barn samt efterleva samtliga krav nedan. Appar som ingår i programmet Avsett för familjer måste alltid efterleva samtliga krav för programmet. Google Play kan avvisa, ta bort eller stänga av appar som anses vara olämpliga för programmet Avsett för familjer.

Krav för Avsett för familjer

1. Appen måste klassificeras som Ingen åldersgräns, Från 10 år eller motsvarande.
2. I frågeformuläret för innehållsklassificering i Google Play Console måste du uppgi korrekta uppgifter om vilka interaktiva element som förekommer i appen, däribland huruvida
 - användare kan interagera eller utbyta information
 - personliga uppgifter som användare har angett delas med tredje part
 - användarens fysiska plats delas med andra användare i appen.
3. Om [Android Speech API](#) används i appen måste RecognizerIntent.EXTRA_CALLING_PACKAGE vara inställt på dess PackageName.
4. Endast [Google Play-certifierade annons-SDK:er](#) får användas i appar.
5. Platsbehörigheter får inte begäras i appar som särskilt riktar sig till barn.
6. Vid förfrågningar om Bluetooth-åtkomst i appen måste [Companion Device Manager \(CDM\)](#) användas om inte appen endast är inriktad på operativsystemsversioner som inte är kompatibla med CDM.

Här följer några exempel på vanliga sorters appar som inte är behöriga för programmet.

- Appar som klassificeras som Ingen åldersgräns men som innehåller annonser för hasardspel.
- Appar för föräldrar eller vårdgivare (t.ex. amningsappar och guider om barns utveckling).
- Guider för föräldrar eller appar för enhetshantering som är avsedda att användas av föräldrar eller vårdgivare.
- Appar som använder en appikon eller en startikon som är olämplig för barn.

Kategorier

Om du blir godkänd för programmet Avsett för familjer kan du välja en programspecifik tilläggskategori som beskriver din app. Här följer de tillgängliga kategorierna för appar som deltar i programmet Avsett för familjer.

Action och äventyr: Actionspel och -appar som omfattar allt från enkla racingspel och sagoäventyr till andra spännande appar och spel.

Hjärngympa: Spel som grundar sig på användarens tankeförmåga, bland annat pussel, matchningsspel, quiz och andra spel som utmanar minnet, intellektet och det logiska tänkandet.

Kreativitet: Appar och spel som uppmuntrar till kreativitet, där användaren till exempel tecknar, målar eller programmerar samt andra appar och spel där man bygger och skapar saker.

Utbildning: Appar och spel som har utformats med hjälp av experter på inläring (t.ex. lärare, pedagoger och forskare) i syfte att uppmuntra till lärande. Detta omfattar till exempel akademisk, social och känslomässig, fysisk och kreativ inläring samt inläring kopplad till grundläggande livkunskap, kritiskt tänkande och problemlösning.

Musik och video: Appar och spel med musik- eller videokomponenter, vilket omfattar allt från appar som simulerar instrument till appar med musik- eller videoinnehåll.

Rollspel: Appar och spel där användaren kan spela en roll och till exempel låtsas vara kock, vårdgivare, prins eller prinsessa, brandman, polis eller en påhittad rollfigur.

Annonser och intäkter

Policyerna nedan gäller för all annonsering i appen, inklusive annonser för dina appar och appar från tredje part, erbjudanden om köp i appen och allt övrigt kommersiellt innehåll (till exempel betald produktplacering) som visas för användare av appar som omfattas av kraven i familjepolicyn och/eller kraven för Avsett för familjer. All annonsering, alla erbjudanden om köp i appar och allt kommersiellt innehåll i dessa appar måste efterleva alla tillämpliga lagar och bestämmelser (inbegripet eventuella relevanta inbördes bestämmelser eller branschriktlinjer).

Google Play förbehåller sig rätten att avvisa, ta bort eller stänga av appar som innehåller alltför påstridiga kommersiella strategier.

Annonssformatkrav

Det får inte förekomma missvisande innehåll i annonser och erbjudanden om köp i appen och de får inte vara utformade på ett sätt som leder till oönskade klick av barn. Följande är förbjudet:

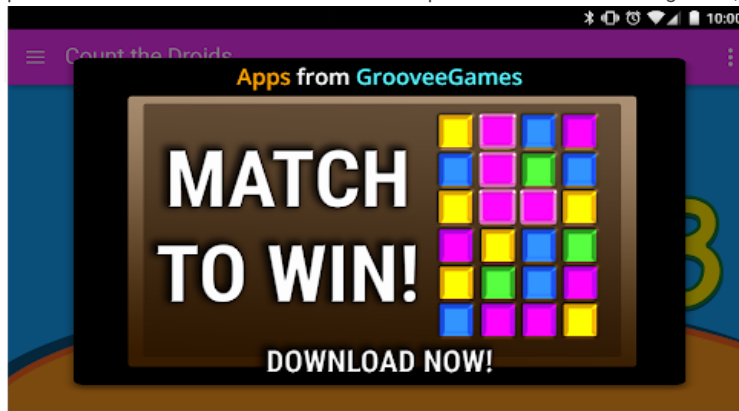
- Störande annonser, inklusive annonser som tar upp hela skärmen eller stör normal användning och som inte har något tydligt sätt att stänga annonsen (t.ex. [annonsväggar](#)).
- Annonser som stör normal användning av appar eller spel och inte går att stänga efter fem sekunder. Annonser som inte stör normal användning av appar eller spel kan visas i mer än fem sekunder (t.ex. videoinnehåll med integrerade annonser).
- Mellansidesannonser eller erbjudanden om köp i appen får inte visas direkt när appen startas.
- Flera annonsplaceringar på en sida (vi tillåter t.ex. inte bannerannonser som visar flera erbjudanden på en placering eller som visar fler än en banner- eller videoannons).
- Annonser eller erbjudanden om köp i appen som inte enkelt kan skiljas från innehållet i appen.
- Användare manipuleras till att titta på annonser eller göra köp i appen med hjälp av känslomässig utpressning eller stötande innehåll.
- Köp i appen som görs med virtuella pengar i spelet kan inte skiljas från köp med riktiga pengar.

Här är några exempel på vanliga överträdelser för annonsformat:

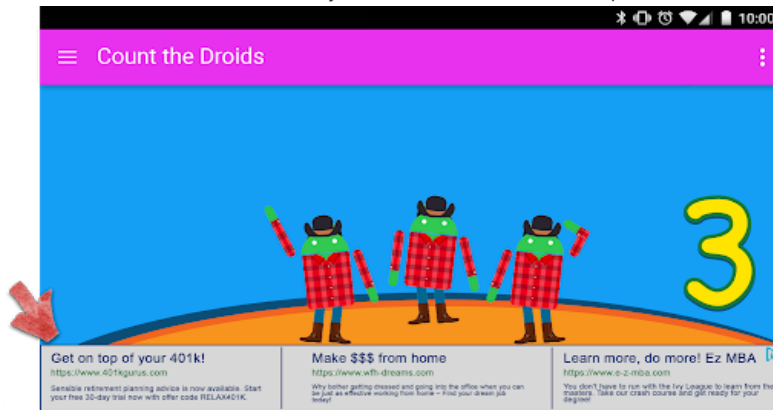
- Annonser som flyttas undan användarens finger när användaren försöker att stänga dem.

- Annonser som tar upp stora delar av skärmen utan att användaren på ett enkelt sätt kan stänga dem, så som visas i

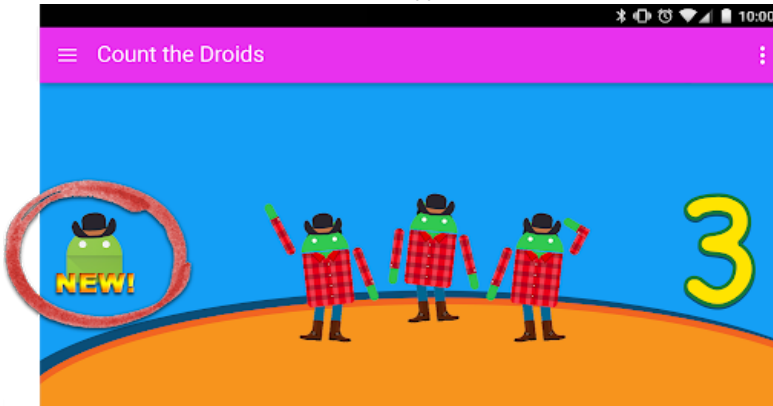
exemplet nedan:



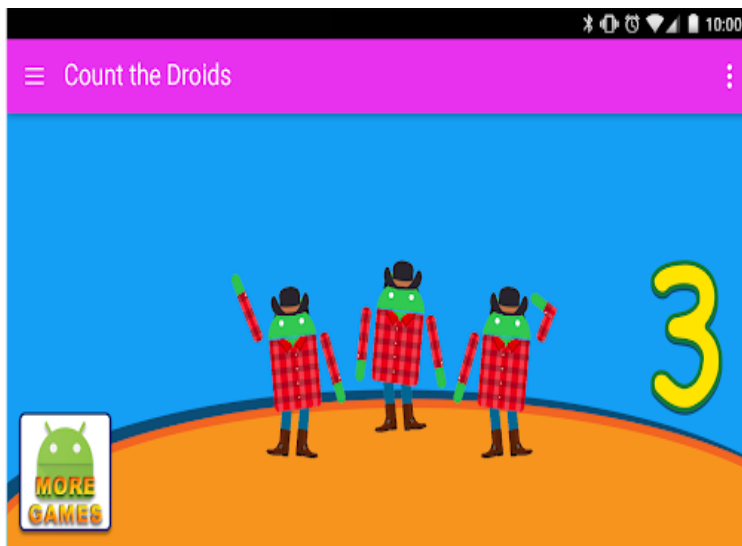
- Bannerannonser som visar flera erbjudanden, så som visas i exemplet nedan:



- Annonser som kan förväxlas med innehåll i appen av användaren, så som visas i exemplet nedan:



- Marknadsföring för dina andra butiksuppgifter i Google Play med hjälp av knappar eller annonser som inte går att skilja från innehåll i appen, så som visas i exemplet nedan:



Här följer några exempel på olämpligt annonsinnehåll som inte ska visas för barn.

- **Olämpligt medieinnehåll:** Annonser för tv-program, filmer, musikalbum eller annan media som är olämplig för barn.
- **Olämpliga tv-spel och nedladdningsbar programvara:** Annonser för nedladdningsbar programvara och elektroniska tv-spel som är olämpliga för barn.
- **Begränsade eller skadliga ämnen:** Annonser för alkohol, tobak, begränsade ämnen eller andra skadliga ämnen.
- **Hasardspel:** Annonser för simulerade hasardspel, tävlingar eller sweepstake-kampanjer, även om det inte kostar något att delta.
- **Barnförbudet eller sexuellt provokativt innehåll:** Annonser med sexuellt, provokativt eller barnförbudet innehåll.
- **Dejting och relationer:** Annonser för webbplatser för dejting eller relationer mellan vuxna.
- **Våldsamt innehåll:** Annonser med våldsamt och explicit innehåll som är olämpligt för barn.

SDK:er för annonser

Om du visar annonser i appen och endast barn ingår i målgruppen måste du använda [Google Play-certifierade annons-SDK:er](#). Om både barn och äldre användare ingår i målgruppen för appen måste du implementera metoder för ålderskontroll, till exempel en [skärm för ålderskontroll](#), och säkerställa att alla annonser som visas för barn endast kommer från Google Play-certifierade annons-SDK:er. Endast självcertifierade annons-SDK:er får användas i appar som ingår i programmet Avsett för familjer.

Mer information om dessa krav och den aktuella listan över godkända annons-SDK:er hittar du i [policyn för programmet för familjeannonser](#).

Om du använder AdMob hittar du mer information om AdMobs produkter i [hjälpcentret för AdMob](#).

Du ansvarar för att säkerställa att appen efterlever alla krav gällande annonsering, köp i appen och kommersiellt innehåll. Kontakta SDK-leverantören om du behöver mer information om deras innehållspolicyer och tillvägagångssätt för annonsering.

Köp i appen

Google Play autentiserar alla användare igen innan några köp i appen sker för appar som deltar i programmet Avsett för familjer. Syftet med åtgärden är att säkerställa att det inte är barn utan parten med det ekonomiska ansvaret som godkänner köpet.

Tillämpning

Det är alltid bättre att undvika att bryta mot policyn än att hantera överträdelsen, men om det ändå händer är det viktigt för oss att utvecklarna förstår hur de kan se till att deras appar följer policyn. Kontakta oss om du [upptäcker några överträdelser](#) eller har frågor om hur du [hanterar en överträdelse](#).

Policyns täckning

Vår innehållspolicy gäller för allt innehåll som din app visar eller länkar till, inklusive annonser som visas för användare och användargenererat innehåll som visas i appen eller som appen länkar till. Den gäller dessutom för allt innehåll från

ditt utvecklarkonto som visas offentligt på Google Play, bland annat ditt utvecklarnamn och målsidan för den angivna utvecklarewebbplatsen.

Vi tillåter inte appar som låter användare installera andra appar på sina enheter. Utvecklare av appar som ger åtkomst till andra appar, spel eller annan programvara utan installation, inklusive funktioner och upplevelser som tillhandahålls av tredje part, måste försäkra sig om att allt innehåll apparna ger åtkomst till följer alla [policyer för Google Play](#). Sådana appar kan även omfattas av ytterligare policygranskningar.

Termerna som används i den här policyn har samma innebörd som i [distributionsavtalet för utvecklare](#). Förutom att följa denna policy och distributionsavtalet för utvecklare måste appens innehåll klassificeras enligt våra [riktlinjer för innehållsklassificering](#).

När vi bedömer om vi ska erbjuda eller ta bort appar från Google Play tar vi hänsyn till ett antal faktorer som omfattar, men inte begränsas till, om det finns ett mönster av skadligt beteende eller en risk för otillåten användning. Vi identifierar risk för otillåten användning utifrån olika omständigheter som omfattar, men inte begränsas till, en tidigare historik med överträdelser, feedback från användare och användning av populära varumärken, figurer och andra tillgångar.

Så här fungerar Google Play Protect

När du installerar appar kontrolleras de via Google Play Protect. Enheten genomsöks även regelbundet. Om en potentiellt skadlig app upptäcks kan följande hända:

- Du kan få en avisering. Du tar bort appen genom att trycka på aviseringen följt av Avinstallera.
- Appen kan inaktiveras tills du avinstallerar den.
- Appen tas bort automatiskt. I de flesta fall när en skadlig app upptäcks får du en avisering om att appen har tagits bort.

Så här fungerar skyddet mot skadlig programvara

För att skydda dig mot skadlig programvara från tredje part, skadliga webbadresser och andra säkerhetsproblem kan Google få information om

- enhetens nätverksanslutningar
- potentiellt skadliga webbadresser
- enhetens operativsystem samt appar som installerats på din enhet via Google Play eller andra källor.

Du kan få en varning från Google om en app eller webbadress verkar vara osäker. Om vi vet att en app eller webbadress är skadlig för enheter, data eller användare kan Google ta bort eller blockera installationen av den.

Du kan välja att inaktivera vissa av dessa skydd i enhetsinställningarna. Men Google kan få information om appar som har installerats via Google Play även i fortsättningen, och appar som har installerats på din enhet från andra källor kan kontrolleras av säkerhetsskäl även i fortsättningen utan att informationen skickas till Google.

Så fungerar integritetsvarningar

Google Play Protect varnar dig om en app tas bort från Google Play Butik därför att appen kan få tillgång till personliga uppgifter, och du ges möjlighet att avinstallera appen.

Tillämpningsprocess

Om appen bryter mot någon av våra policyer vidtar vi lämpliga åtgärder enligt beskrivningen nedan. Vi ger dig dessutom relevant information via e-post om vilka åtgärder vi vidtar tillsammans med anvisningar om hur du överklagar om du anser att vi vidtagit åtgärder på felaktig grund.

Observera att meddelanden om borttagning eller administrativa meddelanden kanske inte tar upp alla enskilda fall av överträdelse av policyn som finns i appen eller appkatalogen. Alla utvecklare ansvarar för att åtgärda policyproblem och för att se till att deras appar i övrigt följer policyn i sin helhet. Ytterligare åtgärder kan vidtas om du inte åtgärdar policyöverträdelser i alla dina appar.

Upprepade eller allvarliga överträdelser (till exempel skadlig programvara, bedrägerier och appar som kan skada användaren eller enheten) av denna policy eller [distributionsavtalet för utvecklare](#) leder till att enskilda eller relaterade utvecklarkonton på Google Play sägs upp.

Tillämpningsåtgärder

Olika tillämpningsåtgärder kan påverka appen på olika sätt. I följande avsnitt beskrivs vilka åtgärder Google Play kan vidta och hur dessa påverkar din app och/eller ditt utvecklarkonto på Google Play. Den här informationen förklaras också

i denna [video](#).

Avvisning

- En ny app eller appuppdatering som skickas in för granskning blir inte tillgänglig på Google Play.
- Om en uppdatering till en befintlig app avvisas är appversionen som publicerades före uppdateringen fortfarande tillgänglig på Google Play.
- Avvisningar påverkar inte åtkomsten till en avvisad apps befintliga användarinstallationer, statistik och betyg.
- Avvisningar påverkar inte statusen för ditt utvecklarkonto på Google Play.

Obs! Försök inte skicka in en avvisad app igen förrän du har åtgärdat alla policyöverträdelser.

Borttagning

- Appen och eventuella tidigare versioner av appen tas bort från Google Play och användarna kan inte längre ladda ned den.
- Eftersom appen tas bort kan användarna inte se appens butiksuppgifter, användarinstallationer, statistik och betyg. Informationen återställs när du skickar in en uppdaterad version av en borttagen app som följer policyn.
- Användare kanske inte kan genomföra köp i appen eller använda faktureringsfunktioner i appen förrän en version som följer policyn har godkänts av Google Play.
- Borttagningar påverkar inte statusen för ditt utvecklarkonto på Google Play omedelbart, men upprepade borttagningar kan leda till avstängning.

Obs! Försök inte publicera en borttagen app på nytt förrän du har åtgärdat alla policyöverträdelser.

Avstängning

- Appen och eventuella tidigare versioner av appen tas bort från Google Play och användarna kan inte längre ladda ned den.
- Avstängning kan genomföras till följd av allvarliga eller åtskilliga policyöverträdelser samt upprepade avvisade eller borttagna appar.
- Eftersom appen är avstängd kan användarna inte se appens butiksuppgifter, befintliga användarinstallationer, statistik och betyg. Informationen återställs när du skickar in en uppdaterad version av en borttagen app som följer policyn.
- Du kan inte längre använda APK-filer eller AAB-arkiv för avstängda appar.
- Användare kanske inte kan genomföra köp i appen eller använda faktureringsfunktioner i appen förrän en version som följer policyn har godkänts av Google Play.
- Avstängningar räknas som varningar och påverkar statusen för utvecklarkontot på Google Play negativt. Flera varningar kan leda till att enskilda och relaterade utvecklarkonton på Google Play sägs upp.

Obs! Försök inte publicera en avstängd app på nytt om inte Google Play har förklarat att du kan göra det.

Begränsad synlighet

- Appens synlighet på Google Play är begränsad. Appen är fortfarande tillgänglig på Google Play och användarna kan komma åt den med en direktlänk till appens butiksuppgifter i Play.
- Att appen har begränsad synlighet påverkar inte statusen för ditt utvecklarkonto på Google Play.
- Att appen har begränsad synlighet påverkar inte användarnas möjlighet att se appens befintliga butiksuppgifter, användarinstallationer, statistik och betyg.

Uppsägning av konto

- När ditt utvecklarkonto sägs upp tas alla appar i din katalog bort från Google Play och du kan inte längre publicera nya appar. Detta innebär också att alla relaterade utvecklarkonton på Google Play stängs av permanent.
- Flera avstängningar, eller avstängningar på grund av allvarliga policyöverträdelser, kan också leda till att Play Console-kontot sägs upp.
- Eftersom apparna i det uppsagda kontot tas bort kan användarna inte se appens butiksuppgifter, befintliga användarinstallationer, statistik och betyg.

Obs! Alla nya konton som du försöker öppna avslutas också (utan återbetalning av registreringsavgiften för utvecklare), så försök inte registrera dig för ett nytt Play Console-konto om ett av dina andra konton sägs upp.

Hantera och rapportera policyöverträdelser

How to handle a policy violation on Go...



Överklaga en tillämpningsåtgärd

Vi återställer appar om det har skett ett misstag och en ny granskning visar att appen inte bryter mot programpolicyen för Google Play och distributionsavtalet för utvecklare. Om du har läst igenom policyerna noggrant och anser att vårt beslut kan ha varit felaktigt följer du anvisningarna i e-postmeddelandet om åtgärderna för att överklaga vårt beslut.

Fler resurser

Om du har frågor om en åtgärd eller ett betyg/en kommentar från en användare hittar du mer information i resurserna nedan. Du kan även kontakta oss via [hjälpcentret för Google Play](#). Vi kan dock inte erbjuda juridisk rådgivning. Om du behöver juridisk rådgivning rekommenderar vi att du kontaktar en jurist.

- [Appverifiering och överklaganden](#)
- [Rapportera en policyöverträdelse](#)
- [Kontakta Google Play om du vill säga upp ett konto eller ta bort en app](#)
- [Skäliga varningar](#)
- [Rapportera olämpliga appar och kommentarer](#)
- [Min app har tagits bort från Google Play](#)
- [Information om uppsägningar av utvecklarkonto för Google Play](#)



Ge feedback om denna artikel

Var det här till hjälp?

Ja

Nej

Behöver du mer hjälp?

Testa detta härnäst:

Kontakta oss

Berätta mer så hjälper vi dig