Programpolicy för utvecklare

(gäller 30 oktober 2024, om inget annat anges)

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 laddar 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 som inte förbjuder andra att skapa, ladda upp eller distribuera innehåll som underlättar exploatering av eller våld mot barn tas omedelbart bort från Google Play. Detta omfattar allt material som visar sexuella övergrepp mot barn. Om du vill anmäla att en Google-produkt har ett innehåll som kan exploatera barn klickar du på **Anmäl otillåten användning** . Om du hittar innehåll på andra ställen på internet bör du kontakta lämplig myndighet i ditt land direkt.

Det är förbjudet att använda appar som utsätter barn för fara. Detta inbegriper men är inte begränsat till användningen av appar som förespråkar exploatering av barn, till exempel

- olämpliga interaktioner riktade mot barn (till exempel tafsande eller smekningar)
- gromning av barn, till exempel att bli vän med ett barn online för att, antingen online eller offline, möjliggöra sexuell kontakt och/eller utbyte av sexuella bilder med barnet
- sexualisering av minderåriga (till exempel bilder som visar, uppmuntrar till eller främjar sexuellt utnyttjande av barn, eller att framställa barn på ett sätt som kan leda till sexuellt utnyttjande av barn)
- utpressning i sexuellt syfte (till exempel att hota eller utpressa ett barn genom att använda verklig eller påstådd åtkomst till ett barns intima bilder)
- trafficking med barn (till exempel annonsering om eller förledande av ett barn för sexuell exploatering i kommersiellt syfte).

Vi vidtar lämpliga åtgärder, vilket kan inbegripa rapportering till National Center for Missing & Exploited Children, om vi upptäcker innehåll med material som visar sexuellt utnyttjande av barn. Om du tror att ett barn är i fara eller har utsatts för övergrepp, exploatering eller trafficking kontaktar du polisen och en barnsäkerhetsorganisation från listan här .

Appar som riktar sig till barn men innehåller barnförbjudna ämnen är inte heller tillåtna, inbegripet men inte begränsat till

- appar med överdrivet våld och blodigt innehåll
- 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, viktminskning och andra kosmetiska förändringar av en persons fysiska utseende.

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. Vi tillåter inte appar eller appinnehåll som verkar marknadsföra eller uppmuntra sexuella aktiviteter mot betalning. Vi tillåter inte appar som innehåller eller uppmuntrar innehåll kopplat till sexuell exploatering eller som distribuerar sexuellt innehåll utan samtycke. Innehåll som visar nakenhet kan vara tillåtet om det syftar till att vara utbildande, dokumentärt, vetenskapligt eller konstnärligt och inte är opåkallat.

Katalogappar – appar som har listor över böcker/videor som en del av en större innehållskatalog – får distribuera böcker (både e-böcker och ljudböcker) eller videor som innehåller sexuellt innehåll förbehållet att följande krav uppfylls:

- Böcker/videor med sexuellt innehåll utgör en liten bråkdel av hela katalogen i appen.
- Böcker/videor med sexuellt innehåll marknadsförs inte aktivt i appen. Dessa titlar kan fortfarande visas i rekommendationer baserat på användarnas historik eller under allmänna priskampanjer.
- Appen distribuerar inte någon bok/video som har innehåll där barn utsätts för fara, porr eller annat sexuellt innehåll som är olagligt enligt tillämpliga lagar.
- Appen skyddar minderåriga genom att begränsa åtkomst till böcker/videor med sexuellt innehåll.

Om en app har innehåll som bryter mot policyn men innehållet i fråga anses vara lämpligt i en viss region kan appen bli tillgänglig för användare i endast den regionen.

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 främjar sexuellt relaterad underhållning, eskorttjänster eller andra tjänster som kan tolkas som att sexuella tjänster erbjuds eller marknadsförs mot betalning i appar, inbegripet men inte begränsat till dejter mot betalning eller sexuella överenskommelser där en deltagare förväntas (implicit eller explicit) att tillhandahålla pengar, gåvor eller finansiellt stöd till den andra parten (så kallad sugardejting).
- Appar som är nedlåtande mot eller objektifierar personer, till exempel genom att påstås kunna se genom klädesplagg eller klä av personer, även om detta presenteras som skämt eller underhållning.
- Innehåll eller beteenden som syftar till att hota eller exploatera människor på ett sexuellt sätt, till exempel smygfoton, dolda kameror, sexuella övergrepp eller sexuellt innehåll utan samtycke som skapats med teknik för deepfake eller liknande.

Hatretorik

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

könsidentitet, kast, invandringsstatus 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 några 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, ätstörningar, strypningslekar eller andra handlingar som kan leda till allvarliga skador eller dödsfall.

Våldsam extremism

Vi tillåter inte att terroristorganisationer, eller andra farliga organisationer eller rörelser som har varit involverade i, förberett eller gjort anspråk på våldshandlingar mot civila, publicerar appar på Google Play i något syfte, inklusive rekrytering.

Vi tillåter inte appar med innehåll som är relaterat till våldsam extremism eller innehåll som är relaterat till planering, förberedelse eller förhärligande av våld mot civila, till exempel innehåll som främjar terroristhandlingar, uppmanar till våld eller hyllar terroristattacker. Om innehåll som är relaterat till våldsam extremism läggs upp i ett pedagogiskt, dokumentärt, vetenskapligt eller konstnärligt syfte är det viktigt att du ger tillräckligt med information om syftet.

Känsliga händelser

Vi tillåter inte appar som tjänar pengar på eller agerar okänsligt inför en känslig händelse av stor social, kulturell eller politisk betydelse, till exempel allmänna nödsituationer, naturkatastrofer, allmänna hälsorelaterade nödsituationer, konflikter, dödsfall eller andra tragiska händelser. 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 några exempel på vanliga överträdelser:

- Okänsligt beteende med avseende på riktiga personers eller gruppers bortgång till följd av självmord, överdos, naturliga orsaker o.s.v.
- Förneka att en väldokumenterad och stor tragisk händelse inträffat.
- Förefalla att dra nytta av en känslig 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 några exempel på vanliga överträdelser:

- mobba 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.
- 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 försäljningen av tobak eller produkter som innehåller nikotin (t.ex. e-cigaretter, vape-pennor och snus) eller som uppmuntrar till olaglig eller olämplig användning av alkohol, tobak eller nikotin.

Ytterligare information

- Skildring av eller uppmuntran till användning eller försäljning av alkohol eller tobak till minderåriga tillåts inte.
- Att antyda att konsumtion av tobak kan förbättra social, sexuell, yrkesmässig, intellektuell eller idrottslig status tillåts inte.
- Positiva framställningar av överdrivet drickande, inbegripet positiva framställningar av måttlöst drickande, hetsdrickande eller drickande i tävlingssyfte tillåts inte.
- Annonser, kampanjer eller framträdande skildringar av tobaksprodukter (inklusive annonser, banners, kategorier och länkar till webbplatser som säljer tobak) tillåts inte.
- Vi kan tillåta begränsad försäljning av tobaksprodukter i hemleveransappar för livsmedel i vissa regioner, med krav på åldersverifieringsåtgärder (t.ex. id-kontroll vid leverans).
- Vi kan tillåta försäljning av produkter för att bli nikotinfri, med krav på åldersverifieringsåtgärder.

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.

Alla appar som innehåller finansiella funktioner måste fylla i deklarationsformuläret för finansiella funktioner i Play Console.

Binära optioner

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

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.
- Exempel som inte ingår: hypotekslån, billån, revolverande krediter (som kreditkort, personliga krediter).

Appar som erbjuder privatlån, inbegripet men inte begränsat till appar som erbjuder lån direkt, genererar potentiella kunder och sätter konsumenter i kontakt med tredje part, måste ställa in Ekonomi som appkategori i Play Console och 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 den huvudsakliga avgiften och alla aktuella avgifter
- en integritetspolicy där åtkomst, insamling, användning och delning av personliga och känsliga användaruppgifter enligt begränsningarna som beskrivs i den här policyn tydligt redovisas.

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

Undantag från den här policyn kan övervägas för appar för privatlån som driver verksamhet i länder där specifika förordningar tillåter sådana kortsiktiga privatlån enligt etablerade regelverk. I dessa sällsynta fall utvärderas undantag i enlighet med tillämpliga lokala lagar och regler i respektive land.

Vi måste kunna konstatera en koppling mellan ditt utvecklarkonto och tillhandahållna licenser eller dokumentation som bevisar att du kan tillhandahålla privatlån. Vi kan begära ytterligare information eller dokument för att bekräfta att ditt konto efterlever alla lokala lagar och regler.

Appar för privatlån eller appar vars huvudsyfte är att förmedla privatlån (dvs. generering av potentiella kunder eller samordnare), hjälpmedelsappar för lån (t.ex. appar för lånberäkning eller långuider) och appar för åtkomst till lön förbjuds att komma åt känsliga uppgifter, till exempel foton eller kontakter. Följande behörigheter är förbjudna:

- Read_external_storage

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

Appar som nyttjar känsliga uppgifter eller API:er omfattas av ytterligare begränsningar och krav. Du hittar mer information i behörighetspolicyn.

Privata högräntelån

I USA tillåter vi inte appar för privatlån med en årlig räntesats (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.

Landsspecifika krav

Appar för privatlån som riktar in sig mot de angivna länderna måste följa ytterligare krav och tillhandahålla ytterligare dokumentation som en del av deklarationen om finansiella funktioner i Play Console. Du måste, på Google Plays begäran, tillhandahålla ytterligare information eller dokument som visar att du följer tillämpliga regler och licenskrav.

1. **Indien**
   - Om du har licensierats av Reserve Bank of India (RBI) för att ge privatlån måste du skicka en kopia av licensen så att vi kan granska den.
   - Om du inte är direkt involverad i aktiviteter som rör utlåningen av pengar och endast tillhandahåller en plattform där banker eller andra finansinstitut än banker lånar ut pengar till kunder måste du uttryckligen uppge detta i deklarationen.
     - Dessutom måste namnen på alla banker och andra finansinstitut än banker tydligt anges i appens beskrivning.
2. **Indonesien**
   - Om appen använder sig av teknikbaserade tjänster för utlåning av pengar i enlighet med OJK-förordningen 77/POJK.01/2016 (som kan ändras från tid till annan) måste du skicka in en kopia på din giltiga licens till oss för granskning.
3. **Filippinerna**
   - Alla finansierings- och utlåningsföretag som erbjuder lån via webbaserade låneplattformar (OLP) måste få ett SEC-registreringsnummer och ett Certificate of Authority-nummer (CA) från Philippines Securities and Exchanges Commission (PSEC).
     - Du måste även ange organisationsnummer, företagsnamn, PSEC-registreringsnummer och CA-nummer för tillstånd att verka som finansierings- eller låneföretag i appens beskrivning.
   - Appar för lånebaserad crowdfunding, till exempel peer-to-peer-utlåning (P2P) eller enligt definitionen som anges i reglerna och förordningarna gällande crowdfunding (CF Rules), måste utföra transaktioner via PSEC-registrerade CF-mellanhänder.
4. **Nigeria**
   - Digitala utlåningsföretag (Digital Money Lenders, DML) måste följa och slutföra LIMITED INTERIM REGULATORY/REGISTRATION FRAMEWORK AND GUIDELINES FOR DIGITAL LENDING, 2022 (som kan ändras från tid till annan) från Federal Competition and Consumer Protection Commission (FCCPC) i Nigeria och erhålla ett verifierbart godkännande från FCCPC.

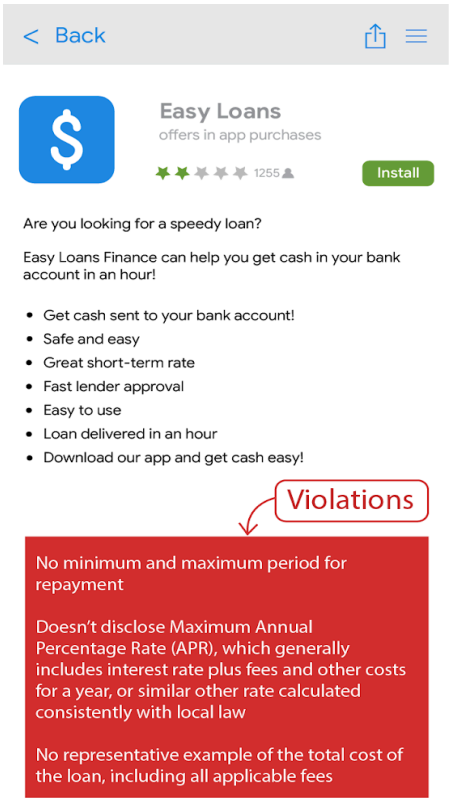
- Låneförmedlare (Loan Aggregators) måste tillhandahålla dokumentation och/eller certifiering för digitala utlåningstjänster och kontaktuppgifter för varje partner-DML.

5. **Kenya**
   - Digitala långivare (Digital Credit Providers, DCP) bör slutföra registreringsprocessen för DCP och erhålla en licens från Kenyas centralbank (CBK). Du måste tillhandahålla en kopia av din licens som en del av deklarationen.
   - Om du inte är direkt involverad i aktiviteter som rör utlåningen av pengar och endast tillhandahåller en plattform där registrerade DCP:er lånar ut pengar till kunder måste du uttryckligen uppge detta i deklarationen och tillhandahålla en kopia av DCP-licensen för respektive partner.
   - I stunden godkänner vi endast deklarationer och licenser från rättssubjekt som har publicerats i Directory of Digital Credit Providers på CBK:s officiella webbplats.

6. **Pakistan**
   - Varje finansinstitut som inte är en bank (NBFC) som lånar ut pengar får bara publicera en (1) digital utlåningsapp (DLA). Utvecklare som försöker publicera flera utlåningsappar per NBFC riskerar att deras utvecklarkonto och eventuella kopplade konton sägs upp.
   - Du måste skicka in bevis på godkännande från SECP för att få erbjuda eller underlätta digitala låntjänster i Pakistan.

7. **Thailand**
   - Appar för privatlån som riktar in sig på Thailand, med räntesatser på 15 % eller högre, måste erhålla en giltig licens från Bank of Thailand (BoT) eller Thailands finansdepartement (MoF). Utvecklare måste tillhandahålla dokumentation som visar att de kan tillhandahålla eller förmedla privatlån i Thailand. Dokumentationen ska innehålla:
     - en kopia av licensen från Bank of Thailand där det framgår att utvecklaren har rätt att driva en privatlånsverksamhet eller en organisation för nanolån
     - en kopia av deras tillstånd att driva en Pico-finanseringsrörelse som utfärdats av finansdepartementet för att kunna vara verksam som Pico- eller Pico-plus-utlånare.

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, bonusprogram med spelliknande drag och appar för daglig fantasysport som uppfyller vissa krav.

Appar med hasardspel

Vi tillåter appar som möjliggör eller underlättar hasardspel online i vissa länder så länge utvecklaren slutför ansökningsprocessen för hasardspelsappar som distribueras i Google Play, är en godkänd statlig operatör och/eller är registrerad som en licensierad operatör hos den ansvariga myndigheten för hasardspel i det angivna landet samt tillhandahåller en giltig operatörslicens i landet i fråga för den typ av produkt för hasardspel online som utvecklaren vill erbjuda. Apparna omfattas dessutom av alla begränsningar och efterlevnadskrav i Google Play-policyerna.

Vi tillåter endast giltiga licensierade eller auktoriserade hasardspelsappar för följande typer av hasardspelsrelaterade produkter online

- Onlinekasinospel
- Sportvadslagning
- Hästkapplöpning (där detta regleras och licensieras separat från sportvadslagning)
- Lotterier
- Daglig fantasysport

Apparna måste uppfylla följande krav:

- Utvecklaren måste genomgå ansökningsprocessen för att distribuera appen på Google 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 eller delstat/territorium där appen distribueras.
- Utvecklaren får inte erbjuda en typ av hasardspel som överskrider omfattningen av licensen för hasardspel.
- Appen måste förhindra att minderåriga använder appen.
- Appen måste förhindra åtkomst och användning i länder, delstater/territorium eller geografiska områden 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 Google 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

För alla andra appar som inte uppfyller ovanstående behörighetskrav för appar med hasardspel och inte ingår i Pilotprogram för andra spel om riktiga pengar nedan tillåter vi 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, sportvadslagning, lotterier och spel som tar emot riktiga pengar och erbjuder kontantpriser eller annat av verkligt värde (förutom de program som tillåts enligt kraven för spelifierade bonusprogram som beskrivs nedan).

Exempel på överträdelser

- Spel som tar emot pengar i utbyte mot en möjlighet att vinna ett fysiskt pris eller ett pris av ekonomiskt värde.

- Appar med navigeringselement eller funktioner (t.ex. menyalternativ, flikar, knappar, WebView med mera) som innehåller en uppmaning till handling som handlar om insatser, satsningar eller deltagande i spel, tävlingar eller turneringar om riktiga pengar, till exempel appar som bjuder in användarna till att SATSA, REGISTRERA SIG eller TÄVLA i en turnering där de kan vinna ett pris i riktiga pengar.
- Appar som tar emot eller hanterar insatser, valutor i appar, vinster eller insättningar i syfte att spela hasardspel för ett fysiskt pris eller ett pris av ekonomiskt värde.

Test för andra spel om riktiga pengar

Det kan hända att vi utför provdrift under en begränsad tid av vissa typer av spel med riktiga pengar i utvalda regioner. Mer information hittar du på den här sidan i hjälpcentret. Provdriften av kloautomatspel online i Japan avslutades den 11 juli 2023. Från och med den 12 juli 2023 kan appar för kloautomatspel online visas globalt på Google Play i enlighet med tillämpliga lagar och vissa krav.

Bonusprogram med spelliknande drag

Om det är tillåtet enligt lag och inte omfattas av ytterligare licenskrav för hasardspel eller spel tillåter vi bonusprogram som belönar användare med fysiska priser eller priser av ekonomiskt värde enligt följande behörighetskrav för Play Butik:

För alla appar (spel och inte spel):

- Fördelar, förmåner och belöningar i bonusprogrammet måste vara supplement till och underordnade kvalificerade monetära transaktioner i appen (där den kvalificerade monetära transaktionen måste vara en genuin separat transaktion för varor eller tjänster som inte är relaterade till bonusprogrammet) och får inte utgöra ett köp eller annars vara kopplat till något slags utbyte som utgör en överträdelse av policyn om hasardspel, spel och tävlingar om riktiga pengar.
  - Till exempel får ingen del av den kvalificerade monetära transaktionen omfatta en avgift eller ersättning för att delta i bonusprogrammet och den kvalificerade monetära transaktionen får inte resultera i köp av varor eller tjänster till ett dyrare pris än vanligt.

För spel -appar:

- Kundpoäng och belöningar med fördelar, förmåner eller belöningar som är kopplade till en kvalificerande monetär transaktion får endast delas ut och lösas in enligt en vinstplan, där vinstandelen dokumenteras tydligt i appen samt i de officiella reglerna för programmet som finns tillgängliga för alla. Dessutom får eventuella intäkter från fördelar eller inlösningsvärden **inte** satsas, delas ut eller öka exponentiellt utifrån spelens resultat eller slumpmässiga utfall.

För appar som inte är spel:

- Kundpoäng eller belöningar kan kopplas till en tävling eller slumpmässiga utfall om de uppfyller kraven nedan. Bonusprogram med fördelar, förmåner eller belöningar som är kopplade till en kvalificerad monetär transaktion måste:
  - Publicera officiella regler för programmet i appen.
  - För program med variabla eller slumpmässiga belöningar ska följande redovisas i programmets officiella villkor: 1) odds, för belöningsprogram med fasta odds, och 2) urvalsmetod (t.ex. vilka variabler som styr belöningen) för alla andra sådana program.
  - Ange fast antal vinnare, fast slutdatum för att delta och datum då priset delas ut, per kampanj, i de officiella villkoren för ett program som erbjuder lottning, vadhållning eller liknande marknadsföring.
  - Om lojalitetspoäng eller bonusbelöningar erhålls och löses in enligt en fast skala ska denna redovisas tydligt i appen liksom i programmets officiella villkor.

Typ av app med bonusprogram	Bonus med spelliknande drag och varierande priser	Bonusbelöningar baserade på en vinstplan/ett regelbundet schema	Användarvillkor för bonusprogram krävs	Användarvillkoren måste redogöra för odds eller urvalsmetod i ett slumpbaserat bonusprogram
Spel	Tillåts ej	Tillåts	Krävs	Inte tillämpligt (spelappar får inte ha slumpmässiga element i bonusprogram)
Inte ett spel	Tillåts	Tillåts	Krävs	Krävs

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

Vi tillåter appar som innehåller annonser med marknadsföring av hasardspel eller spel, tävlingar 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 alla tillämpliga lokala licenskrav 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/prestation eller hantering av betalningar för att delta).
- Appinnehåll får inte marknadsföra eller hänvisa användare till hasardspel eller spel, lotterier eller turneringstjänster med riktiga pengar.

Endast appar som uppfyller alla kraven som nämns i avsnittet (ovan) får innehålla annonser för hasardspel eller spel, lotterier eller turneringar med riktiga pengar. Godkända appar för hasardspel (enligt definitionen ovan) eller godkända appar för daglig fantasysport (enligt definitionen nedan) som uppfyller kraven 1–6 ovan får innehålla annonser för hasardspel eller spel, lotterier eller turneringar med riktiga pengar.

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.
- 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 (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 och ansökningsprocess för hasardspelsappar utanför USA.
- 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.
- 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.
- Appen 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.
- 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 som är synligt eller tillgängligt för åtminstone en del av appens användare.

Appar med användargenererat innehåll, inklusive appar som är särskilt utformade webbläsare eller klienter som omdirigerar användare till en plattform med användargenererat innehåll, måste implementera kraftfull, effektiv och kontinuerlig moderering av det användargenererade innehållet, och de måste göra följande:

- 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 stötande innehåll och beteende (på ett sätt som uppfyller kraven i Google Plays programpolicy för utvecklare) och förbjuda sådant innehåll och beteende i appens användarvillkor eller användarpolicy.
- De måste moderera det användargenererade innehållet på ett sätt som är rimligt och överensstämmer med de typer av användargenererat innehåll som finns i appen. Detta omfattar att

tillhandahålla ett system i appen för att rapportera och blockera stötande användargenererat innehåll och användare samt vidta åtgärder mot användargenererat innehåll och användare vid behov. Olika upplevelser av användargenererat innehåll kan kräva olika modereringar. Exempel:

- Appar med användargenererat innehåll som registrerar en viss grupp av användare genom metoder som användarverifiering och offlineregistrering (till exempel appar som endast används inom en specifik skola eller specifikt företag) måste tillhandahålla en funktion i appen för att rapportera innehåll och användare.
- Funktioner för användargenererat innehåll som tillåter 1:1-användarinteraktion med specifika användare (till exempel direktmeddelanden, taggning och omnämnande) måste tillhandahålla en funktion i appen för att blockera användare.
- Appar som tillhandahåller tillgång till offentligt tillgängligt användargenererat innehåll, som appar för sociala nätverk och bloggappar, måste implementera en funktion i appen för att rapportera användare och innehåll, samt blockera användare.
- 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 sexuellt 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).

- De måste tillhandahålla skyddsåtgärder som förhindrar att intäktsgenerering i appen uppmuntrar användare till olämpligt beteende.

Oförutsett sexuellt innehåll

Sexuellt innehåll anses vara oförutsett om det förekommer i en app med användargenererat innehåll som (1) i första hand ger åtkomst till icke-sexuellt innehåll, och (2) inte aktivt förespråkar eller rekommenderar sexuellt innehåll. Sexuellt innehåll som är olagligt enligt tillämpliga lagar och innehåll där barn utsätts för fara räknas inte som oförutsett och är inte tillåtet.

Appar med användargenererat innehåll får ha oförutsett sexuellt innehåll om alla dessa krav uppfylls:

- Som standard döljs sådant innehåll bakom filter som kräver minst två användaråtgärder för fullständig inaktivering (innehållet kan till exempel döljas bakom en obfuskerad mellansidesannons eller vara dolt som standard om inte säker webbsökning inaktiveras).
- Barns åtkomst till appen (definitionen av barn hittar du i familjepolicyn) är uttryckligen förbjuden genom ålderskontrollsystem, till exempel en skärm för ålderskontroll eller ett system som är lämpligt enligt tillämpliga lagar.
- Du har angett lämpliga svar i frågeformuläret för innehållsklassificering gällande användargenererat innehåll i appen, vilket krävs enligt policyn för innehållsklassificering.

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 sexuellt 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 åtgärda användares klagomål om stötande innehåll.

Hälsorelaterat innehåll och hälsorelaterade tjänster

Vi tillåter inte appar som visar skadligt hälsoinnehåll och skadliga hälsotjänster för användarna.

Om appen innehåller eller marknadsför hälsoinnehåll och -tjänster måste du se till att appen följer gällande lagar och regler.

Hälsoappar

Om appen får åtkomst till hälsodata och antingen är en hälsoapp eller erbjuder hälsorelaterade funktioner måste den följa Google Plays befintliga utvecklarpolicyer, inklusive policyerna för integritet, bedrägeri och otillåten användning samt känsliga händelser, utöver kraven nedan:

- **Console-deklaration:**
  - Öppna sidan Appinnehåll (Policy > Appinnehåll) i Play Console och välj kategorin eller kategorierna som din app tillhör.
- **Krav på integritetspolicy och tydlig redogörelse:**
  - Appen måste ha en länk till integritetspolicyn i det avsedda fältet i Play Console och en länk till integritetspolicyn eller en integritetspolicytext i själva appen. Se till att integritetspolicyn finns tillgänglig via en aktiv webbadress som är tillgänglig för allmänheten och inte är geoblockerad (inga PDF-filer) och att den inte kan redigeras (i enlighet med avsnittet om datasäkerhet).
  - Appens integritetspolicy ska, tillsammans med eventuella meddelanden i appen, tydligt beskriva hur appen kommer åt, samlar in, använder och delar personliga eller känsliga användaruppgifter. Detta ska inte begränsas till data som anges i avsnittet om datasäkerhet ovan. För alla funktioner eller data som regleras av farliga behörigheter eller körningsbehörigheter måste appen uppfylla alla tillämpliga krav på tydlig redogörelse och samtycke.
  - Behörigheter som inte krävs för en hälsoapps huvudfunktion bör inte begäras och oanvända behörigheter måste tas bort. Läs Kategorier av hälsoappar och ytterligare information för att se en lista över alla behörigheter som anses omfatta hälsorelaterade känsliga uppgifter.
  - Om din app inte primärt är en hälsoapp men har hälsorelaterade funktioner och har åtkomst till hälsodata omfattas den fortfarande av policyn för hälsoappar. Kopplingen mellan appens huvudfunktion och insamlandet av hälsorelaterad data (till exempel försäkringsbolag, eller spelappar som samlar in en användares aktivitetsdata för att användaren ska kunna avancera i spelet) ska tydligt framgå för användaren. Denna begränsade användning måste framgå av appens integritetspolicy.
- **Ytterligare krav:**
  Om din hälsoapp uppfyller villkoren för en av följande klassificeringar måste du följa relevanta krav utöver att välja rätt kategori i Play Console:
  - **Hälsoappar med anknytning till myndigheter:** Om du har tillstånd från en myndighet eller en erkänd sjukvårdsorganisation att utveckla och distribuera en app i samarbete med organisationen eller myndigheten måste du skicka in ett bevis på att du uppfyller kraven via förvarningsformuläret.
  - **Appar för kontaktspårning/hälsostatus:** Om din app är en kontaktspårnings- eller hälsostatusapp väljer du Sjukdomsförebyggande och folkhälsa i Play Console och tillhandahåller den obligatoriska informationen via förvarningsformuläret ovan.
  - **Appar för forskning med försökspersoner:** Appar som används till hälsorelaterad forskning med försökspersoner måste följa alla regler och föreskrifter, inbegripet men inte begränsat till att få informerat samtycke av deltagarna eller av en förälder eller vårdnadshavare om deltagaren är minderårig. Hälsoforskningsappar bör även inhämta godkännande från en etikprövningsmyndighet och/eller en motsvarande oberoende etikkommitté såvida de inte är undantagna detta. Bevis på sådant godkännande måste tillhandahållas vid begäran.
  - **Appar för medicintekniska produkter eller för mjukvara för medicintekniska produkter (SaMD-appar):** Appar som anses vara medicintekniska produkter eller SaMD-appar måste erhålla och behålla ett tillståndsbrev eller ett annat dokument för godkännande som har tillhandahållits av en tillsynsmyndighet eller en myndighet ansvarig för styrning av och efterlevnad för hälsoappen. Bevis på sådant tillstånd eller godkännande måste tillhandahållas vid begäran.

Health Connect-data

Data som du kan få åtkomst till med Health Connect-behörighet anses utgöra personliga och känsliga användaruppgifter och omfattas av policyn om användaruppgifter och ytterligare krav .

Receptbelagda läkemedel

Vi tillåter inte appar som underlättar försäljning eller köp av receptbelagda läkemedel utan recept.

Otillåtna ämnen

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

Här är några exempel på vanliga överträdelser:

- 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 .

Felaktig information om hälsa

Vi tillåter inte appar som innehåller vilseledande påståenden om hälsa som motsäger befintlig medicinsk konsensus eller som kan skada andra.

Här är några exempel på vanliga överträdelser:

- Felaktiga påståenden om vacciner, till exempel att vaccin kan förändra någons dna.
- Förespråkande av skadliga, icke godkända behandlingar.
- Förespråkande av andra skadliga vårdmetoder, till exempel konverteringsterapi.

Medicinska funktioner

Vi tillåter inte appar med medicinska eller hälsorelaterade funktioner som är vilseledande eller potentiellt skadliga. Vi tillåter till exempel inte appar som påstår sig ha en syremätningsfunktion men endast är appbaserade. Syremätningsappar måste ha en extern maskinvara, smart accessoar eller dedikerade smartphonesensorer som utformats för att kunna användas med syremätningsfunktioner. De appar som stöds måste också innehålla en ansvarsfriskrivning i sin metadata, där det står att de inte är avsedda för medicinsk användning, att de endast är utformade i allmänna tränings- och hälsosyften och att de inte är medicinsk utrustning. Det måste även finnas tydlig information om vilka maskinvaru- eller enhetsmodeller som är kompatibla.

Betalningar – kliniska tjänster

Google Plays faktureringssystem ska inte användas för transaktioner gällande reglerade kliniska tjänster. Läs mer i Så fungerar Google Plays betalningspolicy .

Blockkedjebaserat innehåll

Samtidigt som blockkedjetekniken utvecklas i snabb takt vill vi tillhandahålla en plattform där utvecklare kan göra framsteg inom innovation och skapa ännu mer berikande och uppslukande upplevelser för användare.

I den här policyn räknar vi blockkedjebaserat innehåll som digitala tokentillgångar som säkrats i en blockkedja. Om din app har blockkedjebaserat innehåll måste du följa dessa krav.

Kryptobörser och mjukvaruplånböcker

Att köpa, inneha eller handla med kryptovalutor ska ske via certifierade tjänster i reglerade rättskipningsområden.

Du måste även följa gällande förordningar i den region eller det land som appen inriktas mot och undvika att publicera appen där dina produkter och tjänster är förbjudna. Google Play kan begära att du tillhandahåller ytterligare information eller dokument om din efterlevnad med tillämpliga regler och licenskrav.

Kryptoutvinning

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.

Insynskrav för att distribuera digitala tokentillgångar

Om appen säljer eller gör det möjligt för användarna att tjäna digitala tokentillgångar måste du ange detta i deklarationsformuläret för ekonomiska funktioner på appinnehållssidan i Play Console.

När du skapar en produkt i en app måste du ange att den representerar en digital tokentillgång i produktinformationen. Läs mer i Skapa produkter i appar.

Du får inte förespråka eller förhärliga eventuella vinster från spel- eller handelsaktiviteter.

Ytterligare krav för NFT-spelifiering

I enlighet med Google Plays policy om hasardspel, spel och tävlingar om riktiga pengar ska spelappar som innehåller digitala tokentillgångar, till exempel NFT:er, genomgå ansökningsprocessen.

För alla andra appar som inte uppfyller behörighetskraven för appar med hasardspel och inte ingår i Pilotprogram för andra spel om riktiga pengar ska ingenting som har ett monetärt värde godkännas i utbyte mot en chans att erhålla en NFT av okänt värde. NFT:er som köps av användare ska användas eller förbrukas i spelet för att förbättra användarens upplevelse eller hjälpa användaren att göra framsteg i spelet. NFT:er får inte användas för att satsa eller spela om pengar för en möjlighet att vinna priser av verkligt ekonomiskt värde (inklusive andra NFT:er).

Här är några exempel på vanliga överträdelser:

- Appar som säljer paket med NFT:er utan att ange det specifika innehållet och värdet på NFT:erna.
- Sociala kasinospel där du betalar för att spela, till exempel spelautomater, som erbjuder NFT:er som vinst.

AI-genererat innehåll

Allteftersom generativa AI-modeller blir mer allmänt tillgängliga för utvecklare kan du ta med dessa modeller i dina appar för att öka engagemanget och förbättra användarupplevelsen. Google Play vill

hjälpa till att säkerställa att AI-genererat innehåll är säkert för alla användare och att feedback från användare används för att främja ansvarsfull innovation.

AI-genererat innehåll

AI-genererat innehåll är innehåll som har skapats av generativa AI-modeller baserat på användarpromptar. Exempel på AI-genererat innehåll är

- text-till-text-konversationschatbotar med generativa AI där funktionen att prata med chatboten är en central funktion i appen
- bilder genererade av AI baserat på promptar med text, bilder eller via rösten.

För att säkerställa användarsäkerheten, och i enlighet med Google Plays policytäckning, måste appar som genererar innehåll med hjälp av AI följa befintliga utvecklarpolicyer i Google Play, inklusive förbud mot och förhindrande av genereringen av begränsat innehåll, som innehåll som möjliggör exploatering eller övergrepp av barn, samt innehåll med vilseledande funktioner.

Appar som genererar innehåll med hjälp av AI måste ha funktioner i appen för att rapportera och flagga stötande innehåll till utvecklare utan att användaren behöver stänga appen. Utvecklare bör använda sig av användarrapporter för att förbättra innehållsfiltrering och moderering i apparna.

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 förfalskade varor i en app skickar du ett meddelande om förfalskningar .

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 skriven dokumentation som bevisar att du har behörighet att använda immateriella rättigheter som tillhör en tredje part i appen eller butiksuppgifterna (t.ex. varumärkesnamn, logotyper och grafiska tillgångar) kontaktar du Google Play-teamet innan du skickar in appen, så att den inte avslås på grund av överträdelser i form av identitetsstöld eller intrång i immateriella rättigheter.

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 vanliga överträdelser:

- 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.

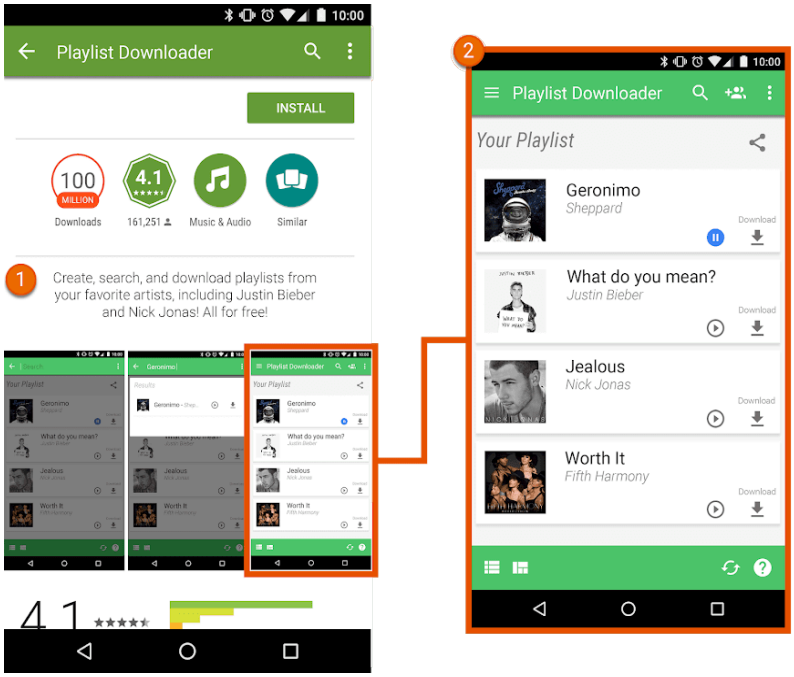
- Reproduktioner eller fan art som inte går att urskilja från upphovsrättsskyddade original.
- Appar där det spelas upp ljudklipp från upphovsrättsskyddat innehåll.
- Fullständiga reproduktioner eller översättningar av böcker som inte är allmän egendom.

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 appuppgifterna uppmuntrar användarna att ladda ned upphovsrättsskyddat material utan tillåtelse.
② Skärmdumpen i appuppgifterna 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 förfalskade varor i appar. Förfalskningar 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.

Användardata

Du måste vara tydlig med hur du hanterar användaruppgifter (till exempel uppgifter som har samlats in från eller om en användare, däribland enhetsinformation). Detta innebär att du ska uppge åtkomst till, insamling, användning, hantering och delning av användaruppgifter i appen och begränsa användningen av uppgifterna till de syften du har angett. Tänk på att all hantering av personliga och känsliga användaruppgifter även omfattas av ytterligare krav i avsnittet om personliga och känsliga användaruppgifter nedan. Dessa krav för Google Play gäller utöver de eventuella krav som föreskrivs i tillämpliga integritets- och dataskyddslagar.

Om du använder kod från tredje part (till exempel ett SDK) i appen måste du se till att koden, och den tredje partens hantering av användaruppgifter, följer Google Plays programpolicy för utvecklare, vilket innefattar krav på användning och redogörelse. Du behöver till exempel se till att dina SDK-leverantörer inte säljer personliga eller känsliga användaruppgifter från appen. Detta krav gäller oavsett om användardatan överförs efter att den skickats till en server eller genom att bädda in koden från tredje part i appen.

Personliga och känsliga användaruppgifter

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, hälsorelaterad data , Health Connect-data , information om vilka övriga appar som finns på enheten, data från mikrofoner och kameror samt övrig känslig enhets- eller användningsinformation. Om appen hanterar personliga eller känsliga användaruppgifter måste du göra följande:

- Begränsa åtkomsten till, insamlingen, delningen och användningen av personliga och känsliga användaruppgifter som har inhämtats via appen till app- och tjänstfunktioner samt i policyefterlevnadssyften som användaren har rimlig anledning att förvänta sig:
  - Appar som utökar användningen av personliga och känsliga användaruppgifter för att visa annonser måste följa Google Plays annonspolicy .
  - Du bör även överföra data som tjänsteleverantörer kräver eller i rättsliga syften som för att följa giltiga förfrågningar från myndigheter, tillämpliga lagar eller vid förvärv eller sammanslagningar, om användarna meddelas på ett juridiskt adekvat sätt.
- Hantera alla personliga och känsliga 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 och känsliga användaruppgifter.
  - Med ”försäljning” menas utbytet eller överföringen av personliga eller känsliga användaruppgifter till en tredje part i monetärt syfte.
    - Användarinitierad överföring av personliga och känsliga användaruppgifter (till exempel när användaren använder en funktion i appen för att överföra en fil till tredje part eller när användaren väljer att använda en undersökningsapp med ett dedikerat syfte) anses inte vara försäljning.

Tydlig redogörelse och krav på samtycke

I de fall där appens åtkomst till, insamling, användning eller delning av personliga och känsliga användaruppgifter kanske inte faller inom vad användaren rimligen förväntar sig av produkten eller funktionen i fråga (till exempel om datainsamlingen pågår i bakgrunden när användaren inte använder appen) måste du uppfylla följande krav:

Tydlig redogörelse: Du måste tillhandahålla en redogörelse i appen för hur du får åtkomst till, 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 integritetspolicy eller i användarvillkoren
- får inte slås ihop med andra redogörelser som inte har koppling till insamling av personliga och känsliga användaruppgifter.

Samtycke och körningsbehörighet: Förfrågningar efter användarnas samtycke i appen och förfrågningar om körningsbehörighet måste direkt föregås av en redogörelse i appen som uppfyller kraven i denna policy. För en begäran om samtycke i appen gäller följande:

- 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.
- Användaren måste ge samtycke innan appen kan börja samla in eller få åtkomst till de personliga och känsliga användaruppgifterna.

Appar som förlitar sig på andra rättsliga grunder för att hantera personliga och känsliga användaruppgifter utan samtycke, som ett berättigat intresse under EU:s GDPR-lagstiftning, måste följa alla tillämpliga rättsliga krav och tillhandahålla lämpliga redogörelser till användarna, till exempel redogörelser i appen som krävs enligt denna policy.

Vi rekommenderar att du följer exempelformatet för tydlig redogörelse (om en sådan krävs) nedan för att efterleva policykraven:

- ”[Denna app] samlar in/överför/synkroniserar/lagrar [datatyp] för att tillhandahålla [”funktion”] [under vilka omständigheter].
- *Exempel: ”Fitness Funds samlar in platsdata för att tillhandahålla träningsresultat, även när appen är stängd eller inte används, samt för annonsering.”*
- *Exempel: ”Call Buddy samlar in samtalshistorik för att möjliggöra kontakt med organisationen även när appen inte används.”*

Om appen använder kod från tredje part (till exempel ett SDK) som är utformad för att samla in personlig och känslig användardata som standard måste du, inom två veckor från att du erhållit en begäran från Google Play (eller om Google Plays begäran tillhandahåller en längre tidsperiod inom den tidsperioden) tillhandahålla tillräckligt bevis på att appen uppfyller kraven på tydlig redogörelse och samtycke enligt denna policy. Detta gäller även med avseende på åtkomst till, insamling, användning eller delning av data via kod från tredje part.

Här är några exempel på vanliga överträdelser:

- Appar som samlar in enhetens plats men saknar en tydlig redogörelse som förklarar vilken funktion som använder uppgifterna och/eller visar appens användning i bakgrunden.

- Appar med körningsbehörighet som begär åtkomst till uppgifter innan en tydlig redogörelse visas som anger vad uppgifterna används till.
- Appar som har åtkomst till användarens lista över installerade appar och inte behandlar dessa uppgifter som personliga eller känsliga uppgifter i enlighet med ovanstående integritetspolicy 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 integritetspolicy 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 använder 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.
- Appar med ett SDK som samlar in personliga och känsliga användaruppgifter och inte behandlar uppgifterna som att de omfattas av denna policy för användaruppgifter och kraven på tydlig redogörelse och samtycke för åtkomst och datahantering (inklusive otillåten försäljning).

Mer information om kraven på tydlig redogörelse och samtycke finns i den här artikeln.

Begränsningar för åtkomst till personliga och 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 och 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 integritetspolicy som tillsammans med eventuella meddelanden i appen förklarar vilka användaruppgifter som samlas in och överförs, hur de används och med vilka parter de delas.
Appen riktar sig till barn	Appen får inte ha ett SDK som inte är godkänt för tjänster som riktar sig till barn. I Utforma appar för barn och familjer kan du läsa om den fullständiga policyn och dess krav.
Appen samlar in eller länkar till beständiga enhetsidentifierare (t.ex. IMEI-kod, IMSI, serienummer för SIM-kort osv.)	Det är inte tillåtet att länka beständiga enhetsidentifierare till personliga eller känsliga användaruppgifter eller enhetsidentifierare som kan återställas, förutom i följande användningsfall: • Telefoni som är kopplad till en identitet för ett SIM-kort (t.ex. wifi-telefoni som är kopplad till ett konto hos en operatör). • Appar för enhetshantering för företag som använder enhetsägarläge. Denna användning måste anges tydligt för användarna i enlighet med specifikationen i policyn om användaruppgifter . Läs mer om andra unika identifierare i den här resursen . I annonspolicyn finns ytterligare riktlinjer om Androids reklam-id.

Avsnitt om datasäkerhet

Alla utvecklare måste fylla i avsnittet om datasäkerhet för varje app tydligt och korrekt och ange information om insamling, användning och delning av användaruppgifter. Utgivaren är ansvarig för att informationen i märkningen stämmer och hålls uppdaterad. Där det är tillämpligt måste avsnittet om datasäkerhet överensstämma med meddelandena i appens integritetspolicy.

Du hittar mer information om hur du fyller i avsnittet om datasäkerhet i den här artikeln .

Integritetspolicy

Alla appar måste ha en integritetspolicy i det avsedda fältet i Play Console och en länk till integritetspolicyn eller en integritetspolicytext i själva appen. Integritetspolicyn ska, tillsammans med eventuella meddelanden i appen, tydligt beskriva hur appen kommer åt, samlar in, använder och delar användaruppgifter. Detta ska inte begränsas till data som anges i avsnittet om datasäkerhet. Detta måste inkludera

- information om utvecklaren och en kontakt för integritetsfrågor eller en mekanism för att skicka in frågor
- redogörelser för de typer av personliga och känsliga användaruppgifter som appen kommer åt, samlar in, använder och delar samt för alla parter som personliga och känsliga användaruppgifter delas med
- processer för säker hantering av personliga och känsliga användaruppgifter
- utvecklarens policy för datalagring och borttagning av data
- en tydlig märkning om integritetspolicy (till exempel kan ordet integritetspolicy användas i rubriken).

Antingen måste enheten (till exempel utvecklaren eller företaget) som namnges i butiksuppgifterna på Google Play vara omnämnd i integritetspolicyn eller så måste appen omnämnas i integritetspolicyn. Även appar som inte får åtkomst till personliga och känsliga användaruppgifter måste ange en integritetspolicy.

Se till att integritetspolicyn finns tillgänglig via en aktiv webbadress som är tillgänglig för allmänheten och inte är geoblockerad (inga PDF-filer) och att den inte kan redigeras.

Krav på borttagning av konto

Om användarna kan skapa ett konto i din app måste den även göra det möjligt för användarna att begära att kontot raderas. Användarna måste ha ett lättillgängligt och synligt alternativ för att initiera borttagning av kontot inifrån appen och utanför den (t.ex. på din webbplats). Det måste finnas en länk till denna webbresurs i det avsedda formulärfältet för webbadresser i Play Console.

När du raderar ett appkonto på begäran från en användare måste du även radera användaruppgifterna som är kopplade till appkontot i fråga. Inaktivering, tillfällig inaktivering eller ”låsning” av appkonton klassas inte som borttagning av konton. Om du behöver behålla vissa uppgifter av giltiga skäl, till exempel av säkerhetsskäl, för att förhindra bedrägeri eller för regelefterlevnad, måste du informera användaren om dina metoder för datalagring (t.ex. i integritetspolicyn).

Om du vill veta mer om kraven på kontoborttagning läser du den här artikeln i hjälpcentret. Du hittar ytterligare information om att uppdatera formuläret för datasäkerhet i den här artikeln.

Användning av appuppsättnings-id

Android lanserar ett nytt id för viktiga användarfall som analyser och för att förhindra bedrägeri. Villkoren för användning av detta id följer nedan.

- **Användning**: Appuppsättnings-id:n får inte användas för annonsanpassning och annonsmätning.
- **Koppling till uppgifter som kan kopplas till en specifik individ och andra identifierare:** Appuppsättnings-id:n får inte kopplas till någon Android-identifierare (t.ex Googles reklam-id) eller några personliga eller känsliga uppgifter i annonssyfte.

- **Insyn och samtycke:** Användarna måste upplysas om att detta appuppsättnings-id används och samlas in och att de här villkoren efterlevs i ett juridiskt adekvat integritetsmeddelande, bland annat i din integritetspolicy. Du måste få användarens juridiskt giltiga samtycke om så krävs. Läs mer om våra integritetsstandarder i policyn om användaruppgifter .

EU-U.S., Swiss Privacy Shield (Privacy Shield-ramverken mellan EU och USA samt Schweiz och USA)

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
- skyddsnivån som krävs enligt uppfyllasekretessprinciperna 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 omedelbart verkan eller vidta rimliga och lämpliga åtgärder för att återställa skyddet till en tillfredsställande nivå.

Sedan den 16 juli 2020 använder Google inte längre EU-U.S. Privacy Shield (Privacy Shield-ramverket mellan EU och USA) vid överföring av personuppgifter med ursprung i Europeiska ekonomiska samarbetsområdet eller Förenade kungariket till USA. (Läs mer.) Mer information finns i avsnitt 9 i Distributionsavtalet.

Behörigheter och API:er med åtkomst till känsliga uppgifter

Förfrågningar om behörighet och API:er med åtkomst till känsliga uppgifter ska vara begripliga för användarna. Du får endast begära behörigheter och API:er med åtkomst till känsliga uppgifter om de krävs för att befintliga funktioner och tjänster i appen som står med i butiksuppgifterna på Google Play ska kunna implementeras. Du får inte använda behörigheter eller API:er med åtkomst till känsliga uppgifter 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 eller API:er med åtkomst till känsliga uppgifter får aldrig säljas eller delas i syfte att underlätta försäljning.

Begär åtkomstbehörighet till uppgifter och till API:er med åtkomst till känsliga uppgifter när de ska användas (med förfrågningar som görs stegvis) 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 är de behörigheter som har markerats med Farlig , Särskild , Signatur eller som beskrivs nedan begränsade. För sådana behörigheter gäller ytterligare krav och begränsningar enligt nedan:

- Användardata eller enhetsinformation som du fått åtkomst till via begränsade behörigheter anses vara personliga och känsliga användaruppgifter. Kraven i policyn för användaruppgifter gäller.
- 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).
- Användning av behörigheter som strider mot Google Plays policyer för skadlig programvara (till exempel otillåten användning av förhöjda behörigheter) är uttryckligen förbjudna.

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 integritets- 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
Behörighetsgruppen Samtalshistorik (t.ex. READ_CALL_LOG, WRITE_CALL_LOG, PROCESS_OUTGOING_CALLS)	Appen måste medvetet ha registrerats som standardhanteraren för telefon och assistans på enheten.
Behörighetsgruppen Sms (t.ex. READ_SMS, SEND_SMS, WRITE_SMS, RECEIVE_SMS, RECEIVE_WAP_PUSH, RECEIVE_MMS)	Den måste medvetet har 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 framhävas i dokumenteringen och lyftas fram i appbeskrivningen. Utan huvudfunktionen går appen sönder 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

Enhetens plats anses utgöra personliga eller känsliga användaruppgifter och omfattas av policyn om personliga och känsliga uppgifter samt av policyn om platsåtkomst i bakgrunden 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 förgrundstjänster (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 .

Du hittar mer information om policykraven i den här hjälpartikeln .

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 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 .

Behörighet att se appaket

Information om vilka appar som finns installerade på en enhet anses utgöra personliga eller känsliga användaruppgifter och omfattas av policyn om personliga och känsliga uppgifter och följande krav:

Appar vars huvudsyfte är att starta, söka efter eller användas ihop med andra appar på enheten kan få behörighet att se andra installerade appar på enheten i den utsträckning som är rimlig enligt beskrivningen nedan:

- **Bred appöverblick:** Med bred överblick avses att appen kan se ett flertal appar (”paket”) som finns installerade på en enhet.
  - Appar som är inriktade på API-nivå 30 eller högre tillåts bara att fråga efter många installerade appar via behörigheten QUERY_ALL_PACKAGES i vissa användningsfall då appen inte fungerar utan kännedom om och/eller möjlighet att samverka med alla andra appar på enheten.
    - Du får inte använda QUERY_ALL_PACKAGES om appen fungerar med en mer preciserad inriktning på vilka paket som behöver vara synliga för den (t.ex. om den kan fråga efter och interagera med enskilda paket snarare än att begära bred överblick).
  - Alternativa metoder att få fram ungefär samma resultat som med behörigheten QUERY_ALL_PACKAGES får också bara användas för den huvudfunktion som användaren ser, och för interaktion med den, hos alla appar som går att upptäcka med metoden ifråga.

  - Läs den här artikeln i hjälpcentret om vilka användningsfall som behörigheten QUERY_ALL_PACKAGES är tillåten för.
- **Begränsad appöverblick:** Med begränsad överblick avses att appen minimerar åtkomsten till data genom att fråga efter ett närmare bestämt urval appar med hjälp av mer preciserade (till skillnad från breda eller ”svepande”) metoder (t.ex. genom att fråga efter enskilda appar som svarar mot deklarationen i appens manifest). Du kan fråga efter appar med den här metoden om din app interagerar med eller hanterar dessa appar på ett sätt som uppfyller policyns krav.
- Möjligheten att se vilka appar som finns installerade på en enhet måste vara direkt relaterad till det huvudsyfte eller den huvudfunktion som användarna ser i appen.

Data om installerade appar som har sökts fram i appar distribuerade via Play får aldrig säljas eller delas i analyssyfte eller för intäktsgenerering via annonser.

Accessibility API

Accessibility API får inte användas till att

- ändra användares inställningar utan tillstånd eller förhindra att användaren inaktiverar eller avinstallerar en app eller tjänst, om inte en förälder eller vårdnadshavare har godkänt det via en föräldrakontrollsapp eller en administratör har godkänt det via programvara för företagshantering
- kringgå Androids inbyggda integritetsinställningar och aviseringar
- ändra eller använda användargränssnittet på ett sätt som är vilseledande eller på något annat sätt strider mot Google Plays utvecklarpolicyer.

Accessibility API har inte utformats för och kan inte begäras för fjärrinspelning av samtalsljud.

Det måste stå att Accessibility API används i butiksuppgifterna på Google Play.

Riktlinjer för IsAccessibilityTool

Appar vars huvudsyfte är att stödja personer med funktionsnedsättning får använda beteckningen **IsAccessibilityTool** för att klassificera sig offentligt som en tillgänglighetsapp.

Appar som inte uppfyller kraven för **IsAccessibilityTool** får inte använda den markeringen, men måste ändå uppfylla kraven på tydligt yppande och samtycke som beskrivs i policyn om användaruppgifter eftersom tillgänglighetssyftet inte är uppenbart för användaren. Du hittar mer information i hjälpcenterartikeln för AccessibilityService API .

Appar måste använda API:er och behörigheter med snävare omfång i stället för Accessibility API om det går att uppnå den önskade funktionen.

Begär behörighet att installera paket

Behörigheten REQUEST_INSTALL_PACKAGES ger en app tillåtelse att begära installation av appaket. Om du vill använda den här behörigheten måste appens huvudfunktion

- inkludera att skicka eller ta emot appaket
- möjliggöra användarinitierade installationer av appaket.

Tillåtna funktioner inkluderar:

- surfa eller söka på webben
- kommunikationstjänster med stöd för bilagor
- delning, överföring eller hantering av filer
- enhetshantering för företag
- säkerhetskopiering och återställning
- enhetsmigrering/överföring mellan telefoner
- tillhörande appar för att synkronisera telefonen med en smart accessoar eller IoT-enhet (till exempel en smartklocka eller smart-tv).

Med appens huvudfunktion avses det som appen i första hand är till för. Huvudfunktionen och eventuella funktioner som ingår i den måste vara klart och tydligt dokumenterade och angivna i appens beskrivning.

Behörigheten REQUEST_INSTALL_PACKAGES får inte användas för att utföra självuppdateringar, modifieringar eller paketering av andra APK:er i tillgångsfilen förutom i enhetshanteringssyfte. Alla uppdateringar eller installationer av paket måste följa Google Plays policy för otillåten användning av enheter och nätverk och måste initieras och genomföras av användaren.

Behörigheter för Health Connect från Android

Health Connect är en Android-plattform som låter appar för hälsa och träning lagra och dela enhetsdata inom ett sammanslaget ekosystem. Den erbjuder en plats där användare kan styra över vilka appar som kan läsa och skriva hälso- och träningsdata. Health Connect har stöd för att läsa och skriva en mängd olika datatyper – allt från steg till kroppstemperatur.

Data som du kan få åtkomst till med Health Connect-behörighet anses utgöra personliga och känsliga användaruppgifter och omfattas av policyn för användaruppgifter. Om din app räknas som en hälsoapp eller har hälsorelaterade funktioner och har åtkomst till hälsodata, inklusive Health Connect-data, måste den även följa policyn för hälsoappar.

Läs mer i den här utvecklarhandboken för Android om hur du kommer igång med Health Connect. Om du vill begära åtkomst till Health Connect-datatyper kan du läsa mer här.

Appar som distribueras via Google Play måste uppfylla följande policykrav för att kunna läsa data från och/eller skriva data till Health Connect.

Lämplig åtkomst till och användning av Health Connect

Health Connect får bara användas i enlighet med tillämpliga policyer, användarvillkor och för godkända användningsfall som har angetts i den här policyn. Det betyder att du bara får begära åtkomst till behörigheter när din app eller tjänst uppfyller villkoren för något av de godkända användningsfallen.

Godkända användningsområden innefattar: träning och hälsa, belöningar, träningscoachning, företagshälsa, sjukvård, hälsoforskning och spel.

Endast appar eller tjänster med en eller flera funktioner vars syfte är att främja användarnas hälsa och träning tillåts begära åtkomst till Health Connect-behörigheter. Det handlar om följande:

- appar eller tjänster som gör det möjligt för användarna **att direkt logga, rapportera, ha koll på och/eller analysera** fysisk aktivitet, sömn, psykisk hälsa, näring, hälsovärden, beskrivningar av kroppen och/eller beskrivningar och mätningar relaterade till hälsa eller träning
- appar eller tjänster som gör det möjligt för användarna **att lagra fysisk aktivitet, sömn, psykisk hälsa, näring, hälsovärden, beskrivningar av kroppen** och/eller beskrivningar och mätningar relaterade till hälsa eller träning på enheten.

Tillgång till Health Connect får inte användas i strid mot denna policy eller andra tillämpliga användarvillkor eller policyer för Health Connect, inklusive i följande fall:

- Använd inte Health Connect i utvecklandet av eller integrering i appar, miljöer eller aktiviteter där användningen eller det felaktiga användandet av Health Connect rimligen kan förväntas leda till dödsfall, personskada, miljöskada eller skada på egendom (som vid uppförandet eller driften av kärnkraftsanläggningar, flygledning, livsuppehållande system eller vapenframställning).
- Begär inte åtkomst till data som erhållits via Health Connect via fönsterlösa appar. Appen måste ha en lätt igenkännlig ikon som visas i appfältet, enhetens appinställningar, aviseringar osv.
- Använd inte Health Connect med appar som synkroniserar data mellan inkompatibla enheter eller plattformar.
- Använd inte Health Connect för att ansluta till appar, tjänster eller funktioner som enbart riktar sig till barn.

- Vidta rimliga och lämpliga åtgärder för att skydda alla appar eller system som använder sig av Health Connect mot obehörig eller olaglig åtkomst, användning, förstörelse, förlust, ändringar eller yppanden.

Det är också ditt ansvar att alla regler och rättsliga krav som gäller följs, baserat på din avsedda användning av Health Connect och all data från Health Connect. Google stöder inte användningen av och kan inte garantera att data som finns i Health Connect för all typ av användning och syfte (i synnerhet gällande användning inom områdena forskning, hälsa och medicin) stämmer, med undantag för när det uttryckligen står på etiketten eller i informationen som Google tillhandahåller för specifika Google-produkter och -tjänster. Google frånsäger sig all ansvarsskyldighet kopplat till data erhållen genom Health Connect.

Begränsad användning

När du använder Health Connect måste åtkomst och användning av data följa vissa begränsningar:

- Dataanvändningen bör vara begränsad till att tillhandahålla eller förbättra lämpliga användningsfall eller funktioner som är synliga i appens användargränssnitt.
- Användaruppgifter får endast överföras till tredje part när användaren uttryckligen har gett samtycke: i säkerhetssyfte (t.ex. för att undersöka otillåten användning), för att följa tillämpliga lagar eller regler eller som en del av sammanslagningar/förvärv.
- Mänsklig åtkomst till användaruppgifter är begränsad såvida användaren inte uttryckligen ger samtycke, i säkerhetssyfte, för att följa lagar eller när de samlas in för intern verksamhet enligt rättsliga krav.
- **All annan överföring, användning eller försäljning av data från Health Connect är förbjuden, till exempel**
  - att överföra eller sälja användaruppgifter till tredje part som annonseringsplattformar, datamäklare eller andra återförsäljare av information
  - att överföra, sälja eller använda användaruppgifter i syfte att visa annonser, inklusive anpassade eller intressebaserade annonser
  - att överföra, sälja eller använda användaruppgifter i syfte att besluta om kreditvärdighet eller för lån
  - att överföra, sälja eller använda användaruppgifter med någon produkt eller tjänst som kan kvalificeras som en medicinteknisk produkt, såvida inte appen för den medicintekniska produkten efterlever alla tillämpliga regler, inklusive att få nödvändiga tillstånd eller godkännanden från relevanta tillsynsorgan (t.ex. FDA i USA) för dess avsedda användning av Health Connect-data, och användaren har gett sitt uttryckliga samtycke för sådan användning
  - att överföra, sälja eller använda användaruppgifter i något syfte eller på ett sätt som involverar Protected Health Information (definierat i HIPAA), om du inte får skriftligt godkännande innan från Google för sådan användning.

Minsta möjliga omfattning

Du får bara begära åtkomst till behörigheterna som behövs för att implementera din produkts funktioner eller tjänster. Sådana åtkomstbegäranden bör vara specifika och begränsade till datan som behövs.

Transparent och exakt meddelande och kontroll

I Health Connect hanteras hälso- och träningsdata, inklusive känsliga uppgifter. Därför måste alla appar ha en omfattande integritetspolicy. Integritetspolicyn måste på ett transparent sätt upplysa om hur appen samlar in, använder och delar användaruppgifter. Utöver rättsliga krav måste utvecklare inkludera följande information i integritetspolicyn:

- en korrekt beskrivning av appens identitet med en sammanfattning av datan som appen har tillgång till och dess koppling till appens viktiga funktioner eller rekommendationer
- praxis för lagring och radering av data

- datahanteringsprocesser (till exempel överföring med modern kryptografi (exempelvis över HTTPS)).

Säker datahantering

Du måste hantera alla användaruppgifter på ett säkert sätt. Vidta rimliga och lämpliga åtgärder för att skydda alla appar eller system som använder sig av Health Connect mot obehörig eller olaglig åtkomst, användning, förstörelse, förlust, ändringar eller yppanden.

Rekommenderade säkerhetsåtgärder är att implementera och underhålla ett hanteringssystem för informationssäkerhet som beskrivs i standarden ISO/IEC 27001. Dessutom bör du säkerställa att appen eller webbtjänsten är stabil och inte har några vanliga säkerhetsproblem enligt OWASP:s topp 10-lista.

Beroende på vilket API som används och antalet användartillåtelser eller användare kräver vi att din app eller tjänst genomgår regelbundna säkerhetsbedömningar och erhåller ett bedömningsintyg från en utsedd tredje part om produkten överför data från användarens egen enhet.

Mer information om krav för appar som kopplas till Health Connect hittar du i denna hjälpartikel.

VPN-tjänst

VpnService är en basklass med vilken appar kan utöka och bygga sina egna VPN-lösningar. Det är bara appar som använder VpnService och har VPN som huvudfunktion som kan skapa en säker tunnel till en fjärrserver på enhetsnivå. Till undantagen räknas appar som kräver en fjärrserver för sin huvudfunktion, till exempel

- föräldrakontroller och appar för företagshantering
- spårning av appanvändning
- appar för enhetssäkerhet (till exempel antivirus, hantering av mobila enheter, brandvägg)
- nätverksrelaterade verktyg (till exempel fjärråtkomst)
- webbläsarappar
- operatörsappar som kräver VPN-funktion för att tillhandahålla telefoni- eller anslutningstjänster.

VpnService kan inte användas för att

- samla in personliga och känsliga användaruppgifter utan tydlig redogörelse och samtycke
- omdirigera eller manipulera användartrafik från andra appar på en enhet i syfte att generera intäkter (till exempel genom att omdirigera annonstrafik via ett annat land än det som användaren befinner sig i)

Appar som använder VpnService måste

- dokumentera användningen av VpnService i uppgifterna på Google Play
- kryptera data från enheten till VPN-tunnelns slutpunkt
- följa alla programpolicyer för utvecklare inklusive policyerna för annonsbedrägeri , behörigheter och skadlig kod .

Behörighet för exakt alarm

Vi introducerar en ny behörighet, USE_EXACT_ALARM, som ger åtkomst till funktioner för exakta alarm i appar från och med Android 13 (API-inriktningsnivå 33).

USE_EXACT_ALARM är en begränsad behörighet och appar får endast deklarera den här behörigheten om det finns stöd för behovet av ett exakt alarm i appens huvudfunktion. Appar som begär den här begränsade behörigheten blir granskade och de som inte uppfyller kriterierna för tillåtna användningsfall får inte publiceras på Google Play.

Tillåtna användningsfall för behörighet att använda exakta alarm

Appen får bara använda USE_EXACT_ALARM-funktionen när appens huvudsakliga, användarriktade funktion kräver att åtgärder sker vid en exakt tid, till exempel när

- appen är en alarm- eller timerapp
- appen är en kalenderapp som visar händelseaviseringar.

Om du har ett användningsfall för en exakt alarmfunktion som inte täcks in av ovanstående kan du överväga om SCHEDULE_EXACT_ALARM kan vara ett alternativ.

Läs mer om funktionen för exakta alarm i riktlinjerna för utvecklare .

Behörighet för helskärmsintent

USE_FULL_SCREEN_INTENT är en behörighet med särskild appåtkomst för appar inriktade på Android 14 (API-inriktningsnivå 34) eller senare. Appar blir bara automatiskt beviljade behörigheten USE_FULL_SCREEN_INTENT om appens huvudfunktion ingår i en av nedanstående kategorier som kräver aviseringar med hög prioritet:

- Ställer in ett alarm
- Tar emot telefon- eller videosamtal

Appar som begär den här behörigheten blir granskade och de som inte uppfyller ovanstående kriterier blir inte automatiskt beviljade den här behörigheten. I sådana fall måste apparna begära behörighet av användaren för att använda USE_FULL_SCREEN_INTENT.

Vi påminner om att all användning av behörigheten USE_FULL_SCREEN_INTENT måste efterleva alla utvecklarpolicyer på Google Play, inklusive våra policyer för oönskad mjukvara på mobila enheter, otillåten användning av enheter och nätverk och annonser. Aviseringar med helskärmsintent får inte störa, skada eller på ett otillåtet sätt få åtkomst till användarens enhet. Dessutom ska appar inte störa andra appar eller enhetens användbarhet.

Läs mer om behörigheten USE_FULL_SCREEN_INTENT i vårt hjälpcenter.

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 eller en programtolk där någon av dem tillhandahåller indirekt åtkomst till Androids API:er (t.ex JavaScript i en WebView eller webbläsare).

Appar eller kod från tredje part (t.ex. SDK:er) med tolkade språk (JavaScript, Python, Lua osv.) som läses in medan de körs (t.ex. om de inte paketerats med appen) får inte möjliggöra eventuella överträdelser av Google Plays policyer.

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:

Exempel på vanliga överträdelser av policyn mot otillåten användning av enheter och nätverk:

- Appar som blockerar eller stör en annan app som visar annonser.
- Fuskappar som påverkar spelandet i andra appar.

- Appar som förmedlar eller ger instruktioner om hur man hackar tjänster, mjukvara eller hårdvara, 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 godkännandelistan 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 (till exempel SDK:er) som laddar ned körbar kod, till exempel dex-filer eller processorkompilerad kod, 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 kod.
- Appar eller kod från tredje part (till exempel SDK:er) med en WebView med ett JavaScript-gränssnitt som läser in osäkert webbinnehåll (t.ex. webbadresser som börjar på http://) eller overifierade webbadresser från osäkra källor (t.ex webbadresser som tillhandahålls av osäkra intent).
- Appar som använder behörigheten för helskärmsintent för att tvinga fram interaktioner med störande annonser eller aviseringar.

Användning av förgrundstjänster

Förgrundstjänstbehörigheten är till för att säkerställa att förgrundtjänster vända mot användaren används på ett lämpligt sätt. För appar som är inriktade på Android 14 eller senare måste du ange en giltig förgrundstjänsttyp för varje förgrundstjänst som du använder i appen och deklarera att förgrundstjänstbehörigheten är lämplig för typen i fråga. Om till exempel geolokalisering på en karta krävs för appens användarfall måste du deklarera behörigheten FOREGROUND_SERVICE_LOCATION i appmanifestet.

Appar får bara deklarera behörigheten för förgrundstjänst om användningen

- gäller en funktion som användaren har nytta av och som hänger ihop med appens huvudfunktion
- initieras av användaren eller är märkbar för användaren (t.ex. ljud från uppspelning av en låt, media som castas till en annan enhet, användaren meddelas tydligt och korrekt, användaren begär att ladda upp ett foto till molnet)
- kan avslutas eller stoppas av användaren
- inte kan avbrytas eller senareläggas av systemet utan att användarupplevelsen påverkas negativt eller en funktion som användaren räknat med inte fungerar som den ska (t.ex. måste ett telefonsamtal starta direkt och kan inte senareläggas av systemet)
- endast pågår så länge som krävs för att slutföra uppgiften.

Användningsfall för förgrundstjänster som undantas från ovanstående kriterier är

- förgrundstjänstetyperna systemExempted eller shortService
- förgrundstjänstetypen dataSync när Play Asset Delivery -funktioner används.

Användningen av förgrundstjänster förklaras mer ingående här.

Användarinitierad dataöverföring

Appar får bara använda API:et för användarinitierad dataöverföring om användningen

- initieras av användaren
- gäller överföringsuppgifter i nätverket
- endast pågår så länge som krävs för att slutföra dataöverföringen.

Användningen av API:er för användarinitierad dataöverföring förklaras mer ingående här.

Flag Secure-krav

FLAG_SECURE är en flagga som anges i en apps kod för att indikera att användargränssnittet innehåller känsliga uppgifter som ska begränsas till en säker plattform medan appen används. Flaggan har utformats för att förhindra att uppgifterna visas på skärmbilder eller osäkra skärmar. Utvecklarna deklarerar den här flaggan när appens innehåll inte ska sändas, visas eller på annat sätt överföras utanför appen eller användarens enhet.

Av säkerhetsskäl och i integritetssyfte måste alla appar som distribueras via Google Play respektera andra appars FLAG_SECURE-deklaration. Det innebär att appar inte får underlätta eller skapa lösningar för att kringgå FLAG_SECURE-inställningarna i andra appar.

Appar som är kvalificerade som tillgänglighetsverktyg undantas från det här kravet så länge de inte överför, sparar eller cachelagrar FLAG_SECURE-skyddat innehåll för användning utanför användarens enhet.

Appar som kör Android-behållare på enheten

Appar med Android-behållare på enheten tillhandahåller miljöer som simulerar hela eller delar av ett underliggande Android OS. Upplevelsen i dessa miljöer kanske inte omfattar den fullständiga uppsättningen med säkerhetsfunktioner i Android. Därför kan utvecklarna välja att lägga till en flagga om säker miljö i manifestet för att signalera till Android-behållare på enheten att de inte ska användas i den simulerade Android-miljön.

Flagga för säker miljö i manifestet

REQUIRE_SECURE_ENV är en flagga som kan deklareras i appmanifestet för att visa att appen inte får köras i Android-behållare på enheten. Av säkerhetsskäl och i integritetssyfte måste appar som tillhandahåller Android-behållare på enheten respektera alla appars deklaration av flaggan och

- leta efter flaggan i manifesten för apparna de tänker läsa in i sin Android-behållare på enheten
- inte läsa in apparna som har deklarerat den här flaggan i sin Android-behållare på enheten
- inte agera proxy genom att spärra eller anropa API:er på enheten så att de ser ut att vara installerade i behållaren
- inte underlätta eller skapa lösningar för att kringgå flaggan (t.ex. genom att läsa in en äldre version av en app för att kringgå den aktuella appens REQUIRE_SECURE_ENV-flagga).

Läs mer om den här policyn i vårt hjälpcenter.

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.

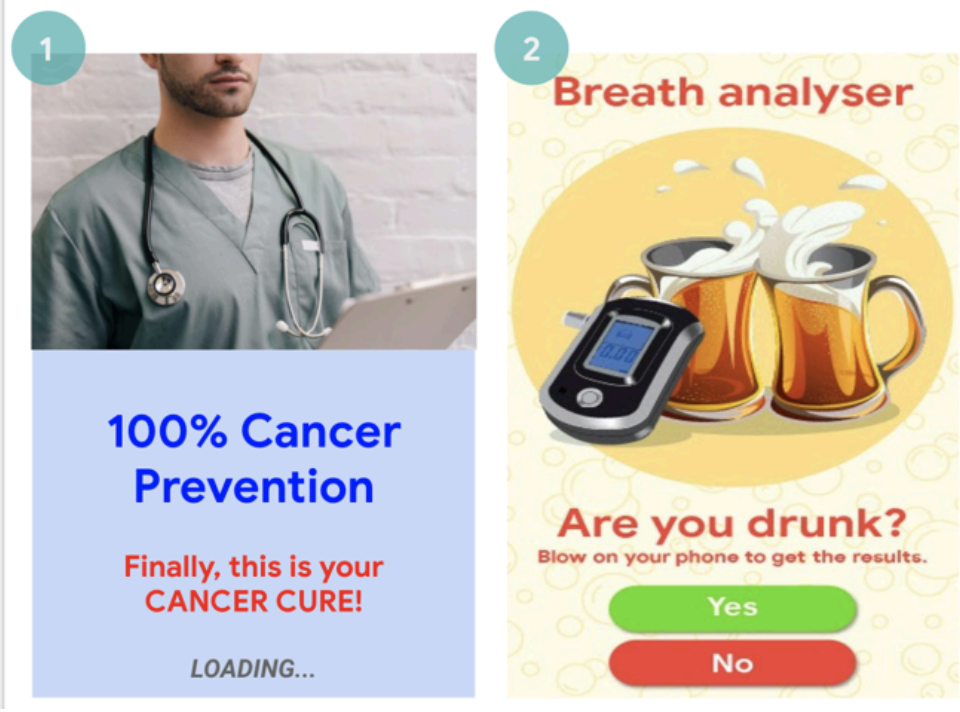
Vilseledande påståenden

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 beskriver sina funktioner på ett missvisande eller otydligt sätt:
  - En app som påstås vara ett racingspel i beskrivningen och skärmbilderna, 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.

- 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 eller falskt innehåll som kan påverka röstningsprocesser eller valresultat.
- Appar som felaktigt påstås ha anknytning till en myndighet eller tillhandahålla eller förmedla myndighetstjänster som appen inte har auktoriserats för.
- Appar som felaktigt utger sig 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 ändrar 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, bankkonton 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 härmar andra appar eller webbplatser för att lura användare att avslöja personuppgifter eller autentiseringsinformation.
- Appar som utan samtycke visar overifierade 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.) och uppdaterar butiksuppgifterna.
- Appar som försöker ändra eller obfuskera funktioner under granskningen.
- Appar där ett nätverk för innehållsleverans (NFI) används för nedladdningar men användaren inte meddelas eller informeras om nedladdningsstorleken före nedladdningen.

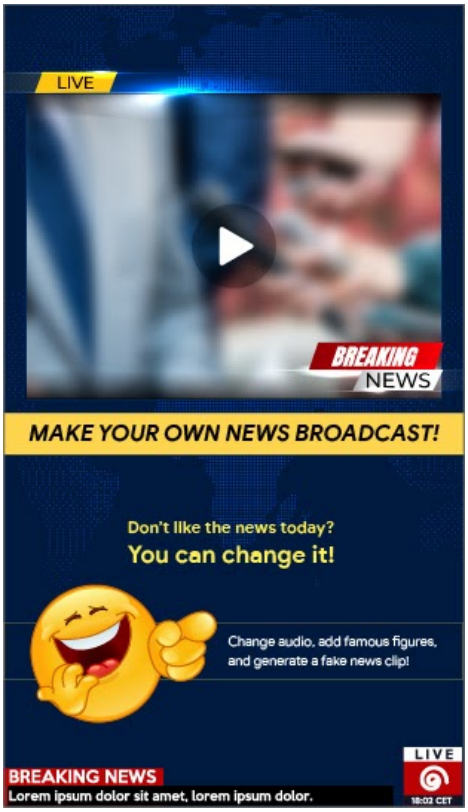
Manipulerad media

Vi tillåter inte appar som främjar eller skapar falsk eller vilseledande information eller påståenden med hjälp av bilder, ljud, 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 redogöra för eller vattenstämpla manipulerad media när 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.

Beteendeinsyn

Appens funktion ska vara rimligt tydlig för användarna. Inkludera inga dolda, inaktiva eller odokumenterade funktioner i appen. Tekniker för att undvika appgranskningar tillåts inte. Appar måste kanske tillhandahålla ytterligare uppgifter för att säkerställa användarsäkerhet, systemintegritet och policyefterlevnad.

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
- som ägnar sig åt samordnade aktiviteter i syfte att vilseleda användare. Detta inbegriper 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.
- samordnar med andra appar, webbplatser, utvecklare eller andra konton för att dölja eller felaktigt framställa identiteten eller annan väsentlig information om utvecklaren eller appen när appinnehållet rör politik, sociala frågor eller frågor av allmänt intresse.

Google Plays policy för API-nivåinriktning

Av säkerhetsskäl krävs följande API-nivåinriktning för **alla appar** på Google Play:

Nya appar och appuppdateringar MÅSTE vara inriktade på en Android API-nivå som lanserats högst ett år från den senaste stora Android-versionen. Nya appar och appuppdateringar som inte uppfyller detta krav kan inte skickas in till Play Console.

Befintliga Google Play-appar som inte har uppdaterats och som inte är inriktade på en API-nivå som lanserats mer än två år från den senaste stora Android OS-versionen kommer inte att vara tillgängliga för nya användare med enheter som kör senare versioner av Android OS. Användare som tidigare har installerat appen från Google Play kan även i fortsättningen hitta, installera om och använda appen på alla Android OS-versioner som appen har stöd för.

I migreringsguiden finns tekniska råd om hur appen uppfyller kraven på API-nivåinriktning.

Du hittar exakta tidslinjer och undantag i den här artikeln i hjälpcentret .

SDK-krav

Apputvecklare använder ofta en kod från tredje part (till exempel ett SDK) för att integrera viktiga funktioner och tjänster i sina appar. När du använder ett SDK i din app måste du se till att du håller användarna och appen skyddade från sårbarheter. I det här avsnittet går vi igenom hur några av våra befintliga krav på integritet och säkerhet gäller för användningen av SDK:er. Kraven är framtagna för att hjälpa utvecklare att integrera SDK:er i sina appar på ett säkert sätt.

Om du använder ett SDK i appen ansvarar du för att den tredje partens kod och praxis inte leder till överträdelser av Google Plays programpolicyer för utvecklare i appen. Det är viktigt att du är medveten om hur SDK:erna i appen hanterar användaruppgifter och att du vet vilka behörigheter som används, vilken data som samlas in och varför. Tänk på att SDK:er måste samla in och hantera användaruppgifter på ett sätt som följer appens användning av uppgifterna i fråga enligt policyn.

Se till att du har läst och förstått de följande policyerna i sin helhet och notera några av de befintliga kraven som gäller för SDK:er nedan så att din användning av SDK:er inte bryter mot policykraven.

Policy för användaruppgifter

Du måste vara tydlig med hur du hanterar användaruppgifter (till exempel uppgifter som har samlats in från eller om en användare, däribland enhetsinformation). Detta innebär att du ska uppge åtkomst till, insamling, användning, hantering och delning av användaruppgifter i appen och begränsa användningen av uppgifterna till de syften du har angett.

Om du använder kod från tredje part (till exempel ett SDK) i appen måste du se till att koden, och den tredje partens hantering av användaruppgifter, följer Google Plays programpolicy för utvecklare, vilket innefattar krav på användning och redogörelse. Du behöver till exempel se till att dina SDK-leverantörer inte säljer personliga eller känsliga användaruppgifter från appen. Detta krav gäller oavsett om användardatan överförs efter att den skickats till en server eller genom att bädda in koden från tredje part i appen.

Personliga och känsliga användaruppgifter

- Begränsa åtkomsten till, insamlingen, delningen och användningen av personliga och känsliga användaruppgifter som har inhämtats via appen till app- och tjänstfunktioner samt i policyefterlevnadssyften som användaren har rimlig anledning att förvänta sig:
  - Appar som utökar användningen av personliga och känsliga användaruppgifter för att visa annonser måste följa Google Plays annonspolicy.
- Hantera alla personliga och känsliga 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.

Försäljning av personliga och känsliga användaruppgifter

Sälj inte personliga och känsliga användaruppgifter.

- Med ”försäljning” menas utbytet eller överföringen av personliga eller känsliga användaruppgifter till en tredje part i monetärt syfte.
  - Användarinitierad överföring av personliga och känsliga användaruppgifter (till exempel när användaren använder en funktion i appen för att överföra en fil till tredje part eller när användaren väljer att använda en

undersökningsapp med ett dedikerat syfte) anses inte vara försäljning.

Krav på tydlig redogörelse och samtycke

I de fall där appens åtkomst till, insamling, användning eller delning av personliga och känsliga användaruppgifter kanske inte faller inom vad användaren rimligen förväntar sig av produkten eller funktionen i fråga måste du uppfylla kraven om tydlig redogörelse och samtycke i policyn för användaruppgifter.

Om appen använder kod från tredje part (till exempel ett SDK) som är utformad för att samla in personlig och känslig användardata som standard måste du, inom två veckor från att du erhållit en begäran från Google Play (eller om Google Plays begäran tillhandahåller en längre tidsperiod inom den tidsperioden) tillhandahålla tillräckligt bevis på att appen uppfyller kraven på tydlig redogörelse och samtycke enligt denna policy. Detta gäller även med avseende på åtkomst till, insamling, användning eller delning av data via kod från tredje part.

Tänk på att se till att koden från tredje part (till exempel ett SDK) inte leder till att appen bryter mot policyn för användaruppgifter.

Du hittar mer information om kraven på tydlig redogörelse och samtycke i den här artikeln i hjälpcentret.

Exempel på överträdelser orsakade av SDK:er

- Appar med ett SDK som samlar in personliga och känsliga användaruppgifter och inte behandlar uppgifterna som att de omfattas av denna policy för användaruppgifter och kraven på tydlig redogörelse och samtycke för åtkomst och datahantering (inklusive otillåten försäljning).
- Appar med ett integrerat SDK som samlar in personliga och känsliga användaruppgifter som standard och bryter mot kraven om användarsamtycke och tydlig redogörelse i den här policyn.
- Appar med ett SDK som förespeglas samla in personliga och känsliga användaruppgifter i syfte att förhindra bedrägeri och otillåten användning i appen, men som även delar uppgifterna som samlas in med tredje part i annons- eller analyssyfte.
- Appar som använder ett SDK som överför information om användarnas installerade paket utan att uppfylla riktlinjerna om tydlig redogörelse och/eller integritetspolicyn.
  - Läs mer i policyn för oönskad mjukvara på mobila enheter.

Ytterligare krav för åtkomst till personliga och känsliga användaruppgifter

I tabellen nedan anges kraven för specifika aktiviteter.

Aktivitet	Krav
Appen samlar in eller länkar till beständiga enhetsidentifierare (t.ex. IMEI-kod, IMSI, serienummer för SIM-kort osv.)	Det är inte tillåtet att länka beständiga enhetsidentifierare till personliga eller känsliga användaruppgifter eller enhetsidentifierare som kan återställas, förutom i följande användningsfall: • Telefoni som är kopplad till en identitet för ett SIM-kort (t.ex. wifi-telefoni som är kopplad till ett konto hos en operatör). • Appar för enhetshantering för företag som använder enhetsägarläge. Denna användning måste anges tydligt för användarna i enlighet med specifikationen i policyn om användaruppgifter . Läs mer om andra unika identifierare i den här resursen . I annonspolicyn finns ytterligare riktlinjer om Androids reklam-id.
Appen riktar sig till barn	Appen kanske bara har SDK:er som är självcertifierade för användning i tjänster som riktar sig till barn. Du kan läsa hela policyn och alla kraven i programmet för självcertifierade annons-SDK:er för familjer.

Exempel på överträdelser orsakade av SDK:er

- Appar som använder ett SDK som länkar Android-id till plats
- Appar med ett SDK som kopplar AAID till beständiga enhetsidentifierare i annons- eller analyssyfte.
- Appar som använder ett SDK som kopplar AAID till e-postadresser i analyssyfte.

Avsnitt om datasäkerhet

Alla utvecklare måste fylla i avsnittet om datasäkerhet för varje app tydligt och korrekt och ange information om insamling, användning och delning av användaruppgifter. Detta inbegriper data som samlas in och hanteras via tredjepartsbibliotek eller SDK:er som används i apparna. Utgivaren är ansvarig för att informationen i märkningen stämmer och hålls uppdaterad. Där det är tillämpligt måste avsnittet om datasäkerhet överensstämma med meddelandena i appens integritetspolicy.

Du hittar mer information om hur du fyller i avsnittet om datasäkerhet i den här artikeln i hjälpcentret.

Läs hela policyn för användaruppgifter.

Policyn för behörigheter och API:er med åtkomst till känsliga uppgifter

Förfrågningar om behörighet och API:er med åtkomst till känsliga uppgifter ska vara begripliga för användarna. Du får endast begära behörigheter och API:er med åtkomst till känsliga uppgifter om de krävs för att befintliga funktioner och tjänster i appen som står med i butiksuppgifterna på Google Play ska kunna implementeras. Du får inte använda behörigheter eller API:er med åtkomst till känsliga uppgifter 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 eller API:er med åtkomst till känsliga uppgifter får aldrig säljas eller delas i syfte att underlätta försäljning.

Läs hela policyn för behörigheter och API:er med åtkomst till känsliga uppgifter.

Exempel på överträdelser orsakade av SDK:er

- Appen använder ett SDK som begär åtkomst till plats i bakgrunden för otillåtna eller okända syften.
- Appen använder ett SDK som överför IMEI-kod som härrör från Android-behörigheten read_phone_state utan användarens samtycke.

Policy om skadlig kod

Vår policy om skadlig kod är enkel: ingen skadlig kod 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.

All kod som kan utgöra en risk för användare, användarnas data eller enheter räknas som skadlig kod. Skadlig kod 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.

Kraven i denna policy gäller även för all kod från tredje part (t.ex. ett SDK) som du inkluderar i appen.

Läs hela policyn om skadlig programvara.

Exempel på överträdelser orsakade av SDK:er

- Appar som använder SDK-bibliotek från leverantörer som distribuerar skadlig mjukvara.
- Appar som inte följer Androids behörighetsmodell eller stjäl 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 använder ett SDK som bryter mot Androids behörighetsmodell genom att skaffa sig förhöjda behörigheter med hjälp av åtkomst till enhetsdata i okänt syfte.
- Appar som använder ett SDK med kod som lurar användarna att prenumerera eller köpa innehåll via telefonräkningen.

Användning av SDK:er i appar

Om du använder ett SDK i appen ansvarar du för att den tredje partens kod och praxis inte leder till överträdelser av Google Plays programpolicyer för utvecklare i appen. Det är viktigt att du är medveten om hur SDK:erna i appen hanterar användaruppgifter och att du vet vilka behörigheter som används, vilken data som samlas in och varför.

SDK-krav

Apputvecklare använder ofta en kod från tredje part (till exempel ett SDK) för att integrera viktiga funktioner och tjänster i sina appar. När du använder ett SDK i din app måste du se till att du håller användarna och appen skyddade från sårbarheter. I det här avsnittet går vi igenom hur några av våra befintliga krav på integritet och säkerhet gäller för användningen av SDK:er. Kraven är framtagna för att hjälpa utvecklare att integrera SDK:er i sina appar på ett säkert sätt.

Om du använder ett SDK i appen ansvarar du för att den tredje partens kod och praxis inte leder till överträdelser av Google Plays programpolicyer för utvecklare i appen. Det är viktigt att du är medveten om hur SDK:erna i appen hanterar användaruppgifter och att du vet vilka behörigheter som används, vilken data som samlas in och varför. Tänk på att SDK:er måste samla in och hantera användaruppgifter på ett sätt som följer appens användning av uppgifterna i fråga enligt policyn.

Se till att du har läst och förstått de följande policyerna i sin helhet och notera några av de befintliga kraven som gäller för SDK:er nedan så att din användning av SDK:er inte bryter mot policykraven.

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

Spionprogram

Spionprogram är skadliga appar, skadlig kod eller skadligt beteende som samlar in, stjäl eller delar användaruppgifter eller enhetsdata som inte rör funktioner som är tillåtna enligt policy.

Skadlig kod eller skadligt beteende som kan betraktas som spionage på användaren eller stöld av data utan lämpligt meddelande eller samtycke anses också vara spionprogram.

Läs hela policyn för spionprogram.

Spionprogramsöverträdelser som orsakas av SDK omfattar men är inte begränsade till följande:

- appar som använder ett SDK som överför data från ljud- eller samtalsinspelningar när det inte har någon koppling till appfunktioner som tillåts enligt policyn
- appar med skadlig kod från tredje part (t.ex. ett SDK) som överför data från enheten på ett sätt som inte förväntas av användaren och/eller utan lämpligt meddelande eller samtycke.

Policy för oönskad mjukvara på mobila enheter

Insyn och tydlig redogörelse

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

Exempel på överträdelser:

- Annonsbedrägeri
- Social manipulering

Skydda användaruppgifter

Var tydlig med hur du kommer åt, använder, samlar in och delar personliga och känsliga användaruppgifter. Användningen av användaruppgifter måste iaktta alla relevanta policyer om

användaruppgifter, om tillämpliga, och vidta alla försiktighetsåtgärder i syfte att skydda sådana uppgifter.

Exempel på överträdelser:

- Datainsamling (se Spionprogram)
- Otillåten användning av begränsade behörigheter

Läs hela policyn om oönskad mjukvara på mobila enheter

Policy för 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.

Appar eller kod från tredje part (t.ex. SDK:er) med interpreterat språk (JavaScript, Python, Lua osv.) som läses in medan de körs (t.ex. om de inte paketerats med appen) får inte möjliggöra eventuella överträdelser av Google Plays policyer.

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.

Läs hela policyn för otillåten användning av enheter och nätverk.

Exempel på överträdelser orsakade av SDK:er

- Appar som underlättar proxytjänster till tredje part får endast göra så om detta är appens primära och grundläggande syfte som visas för användarna.
- Appen använder ett SDK som laddar ned körbar kod, till exempel dex-filer eller processorkompilerad kod, från en annan källa än Google Play.
- Appen använder ett SDK som har en WebView med ett JavaScript-gränssnitt som läser in osäkert webbinnehåll (t.ex. webbadresser som börjar på http://) eller overifierade webbadresser från osäkra källor (t.ex webbadresser som tillhandahålls av osäkra intent).
- Appen använder ett SDK som innehåller kod för att uppdatera sin egen APK-fil.
- Appen använder ett SDK som utsätter användarna för säkerhetssårbarheter genom att ladda ned filer via osäkra anslutningar.
- Appen använder ett SDK som innehåller kod för att ladda ned eller installera appar från okända källor utanför Google Play.
- Appen använder ett SDK som använder förgrundstjänster utan lämpligt användningsfall.
- Appen använder ett SDK som använder förgrundstjänster i enlighet med policyn, men det har inte deklarerats i appens manifest.

Policy för 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.

Läs hela policyn om vilseledande funktioner.

Beteendeinsyn

Appens funktion ska vara rimligt tydlig för användarna. Inkludera inga dolda, inaktiva eller odokumenterade funktioner i appen. Tekniker för att undvika appgranskningar tillåts inte. Appar måste

kanske tillhandahålla ytterligare uppgifter för att säkerställa användarsäkerhet, systemintegritet och policyefterlevnad.

Exempel på en överträdelse orsakad av ett SDK

- Appen använder ett SDK som använder tekniker för att undvika appgranskningar.

Vilka av Google Plays utvecklarpolicyer utsätts mest för överträdelser orsakade av SDK:er?

Som en hjälp för dig att säkerställa att all kod från tredje part som används i din app följer Google Plays programpolicy för utvecklare bör du läsa följande policyer i sin helhet:

- Policyn för användaruppgifter
- Behörigheter och API:er med åtkomst till känsliga uppgifter
- Otillåten användning av enheter och nätverk
- Skadlig kod
- Oönskad mjukvara på mobila enheter
- Programmet för självcertifierade annons-SDK:er för familjer
- Annonspolicyn
- Vilseledande funktioner
- Google Plays programpolicy för utvecklare

De här policyerna bryts det mest emot, men det är viktigt att tänka på att dålig SDK-kod kan leda till att din app bryter mot andra policyer som inte nämns ovan. Kom ihåg att läsa och hålla dig uppdaterad om alla policyer i deras helhet. Det är ditt ansvar som apputvecklare att se till att SDK:erna du använder hanterar appdata på ett sätt som efterlever policyerna.

Du kan läsa mer i vårt hjälpcenter.

Skadlig programvara

Vår policy om skadlig kod är enkel: ingen skadlig kod 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.

All kod som kan utgöra en risk för användare, användarnas data eller enheter räknas som skadlig kod. Skadlig kod 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.

Kraven i denna policy gäller även för all kod från tredje part (t.ex. ett SDK) som du inkluderar i appen.

Skadlig kod 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 kod 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 samlar in personliga eller känsliga användaruppgifter från en enhet och överför uppgifterna till en tredje part (företag eller individ) i övervakningssyfte.

Appar måste tillhandahålla en korrekt och tydlig redogörelse och inhämta samtycke i enlighet med policyn för användaruppgifter .

Riktlinjer för övervakningsappar

Appar som utformats och marknadsförts för övervakning av en annan individ, till exempel för föräldrar som vill övervaka sina barn eller företag som vill övervaka enskilda anställda, är de enda godkända övervakningsapparna, förutsatt att apparna uppfyller alla nedanstående krav. Dessa appar får inte användas till att spåra någon annan (till exempel en partner) även med personens vetskap och samtycke oavsett om en beständig avisering visas. Dessa appar måste använda metadataflaggan IsMonitoringTool i manifestfilen för att klassificera sig själva som övervakningsappar.

Övervakningsappar måste följa dessa krav:

- Appar får inte presenteras som lösningar för spionerі eller hemlig övervakning.
- Appar får inte dölja spårningsbeteende eller försöka vilseleda användare om sådana funktioner.
- Appar måste visa en beständig avisering för användarna när appen körs och en unik ikon som tydligt identifierar appen.
- Appar måste ange övervaknings- eller spårningsfunktionen i butiksbeskrivningen på Google Play.
- Appar och appinformation på Google Play får inte innehålla funktioner som aktiverar eller ger åtkomst till funktioner som bryter mot dessa villkor, till exempel länkar till APK-filer utanför Google Play som inte följer villkoren.
- Appar måste följa gällande lagar. Du är själv ansvarig för att avgöra om appen är laglig i det land eller på den plats där den finns tillgänglig.

Referera till artikeln om användningen av flaggan isMonitoringTool i hjälpcentret för mer information.

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 stjäl 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

Spionprogram är skadliga appar, skadlig kod eller skadligt beteende som samlar in, stjäl eller delar användaruppgifter eller enhetsdata som inte rör funktioner som är tillåtna enligt policy.

Skadlig kod eller skadligt beteende som kan betraktas som spionage på användaren eller stöld av data utan lämpligt meddelande eller samtycke anses också vara spionprogram.

Spionprogramsöverträdelser omfattar men är inte begränsade till följande:

- inspelning av ljud eller inspelning av samtal till telefonen
- stöld av appdata
- appar med skadlig kod från tredje part (t.ex. ett SDK) som överför data från enheten på ett sätt som inte förväntas av användaren och/eller utan lämpligt meddelande eller samtycke.

Alla appar måste även följa Google Plays programpolicy för utvecklare, inklusive policyerna för användaruppgifter och enhetsdata, t.ex. oönskad mjukvara på mobila enheter, användaruppgifter, behörigheter och API:er med åtkomst till känsliga uppgifter och SDK-krav.

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.

Maskware

En app som utnyttjar olika undvikandetekniker för att visa användaren andra eller falska appfunktioner. Dessa appar maskeras som legitima appar eller spel för att verka oskadliga för appbutiker och använder tekniker som obfuskering, dynamisk kodinläsning eller cloaking för att visa skadligt innehåll.

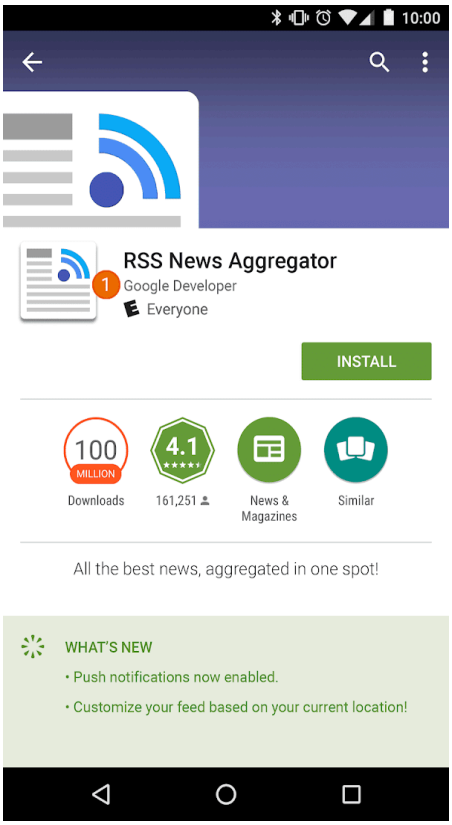
Maskware liknar andra kategorier av potentiellt skadliga appar, i synnerhet trojaner. Den huvudsakliga skillnaden är tekniken som används för att obfuskera den skadliga aktiviteten.

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.

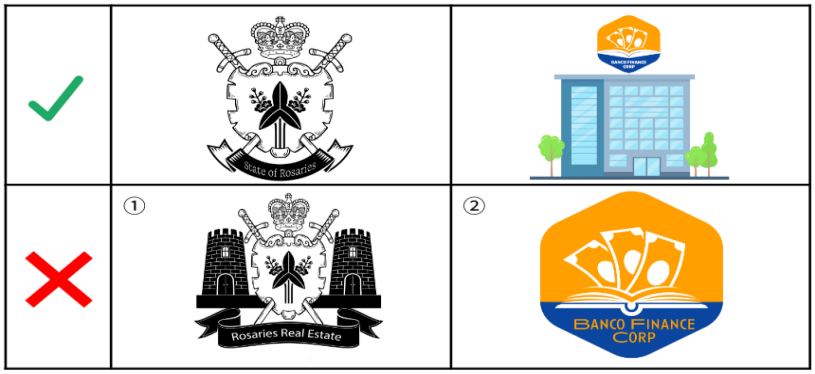
Här är några exempel på vanliga överträdelser:

- Utvecklare som ger falska påståenden om koppling till ett annat företag/en annan utvecklare/enhet/organisation.



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

- Appar med ikoner och rubriker som ger falska påståenden om koppling till ett annat företag/en annan utvecklare/enhet/organisation.



①Appen använder ett nationellt emblem och får användare att tro att den är kopplad till en myndighet.
②Appen kopierar ett företags logotyp, vilket antyder att det är företagets officiella app trots att det inte stämmer.

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

①Appen använder logotypen för en populär webbplats för kryptovaluta i appikonen, vilket antyder att det är den officiella webbplatsen.
②Appen kopierar en karaktär och titel från ett välkänt tv-program i appikonen och får användarna att tro att den har en koppling till tv-programmet trots att det inte stämmer.

- Appar som felaktigt utger sig för att vara officiella appar för etablerade rättssubjekt. Titlar som Justin Bieber Official får inte användas utan tillåtelse eller rättigheter.
- Appar som bryter mot Androids riktlinjer för varumärkning .

Oönskad programvara på mobila enheter

Vi på Google tror att allt annat kommer på köpet om vi väljer att fokusera på användaren. I våra mjukvaruprinciper och vår policy om oönskad mjukvara finns allmänna rekommendationer för mjukvara som ger en bra användarupplevelse. Denna policy bygger vidare på Googles policy om oönskad mjukvara genom att beskriva principerna för Androids ekosystem och Google Play Butik. Mjukvara som strider mot dessa principer kan vara skadlig för användarupplevelsen och vi vidtar åtgärder för att skydda användare mot sådan mjukvara.

Som vi nämnde i policyn om oönskad mjukvara har vi sett att de flesta oönskade mjukvaror har en eller flera av samma grundläggande egenskaper:

- De är vilseledande och ger ett värdeerbjudande som de inte kan hålla.
- Användaren luras att installera mjukvaran 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 mjukvara utan att nämnas.

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

Nedan bygger vi vidare på policyn om oönskad mjukvara i syfte att utöka dess tillämpning till mjukvara på mobila enheter. Precis som med den tidigare nämnda policyn fortsätter vi att finjustera policyn om oönskad mjukvara 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
- Social manipulering

Skydda användarens uppgifter och integritet

Var tydlig med hur du kommer åt, använder, samlar in och delar personliga och känsliga användaruppgifter. Användningen av användaruppgifter måste iaktta alla relevanta policyer för användaruppgifter, om tillämpliga, och vidta alla försiktighetsåtgärder i syfte att skydda sådana uppgifter.

Alla appar måste följa Google Plays programpolicy för utvecklare, inklusive policyerna för användaruppgifter och enhetsdata, t.ex. användaruppgifter, behörigheter och API:er med åtkomst till känsliga uppgifter, spionprogram och SDK-krav.

- Be eller vilseled inte användarna till att inaktivera enhetsskydd som Google Play Protect. Du får till exempel inte erbjuda ytterligare appfunktioner eller belöningar till användare i utbyte mot att de inaktiverar Google Play Protect.

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 mjukvara 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

Fientliga nedladdare

Kod som i sig inte är oönskad programvara men som laddar ned annan oönskad programvara på mobila enheter.

Koden kan vara en fientlig nedladdare om

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

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

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

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:

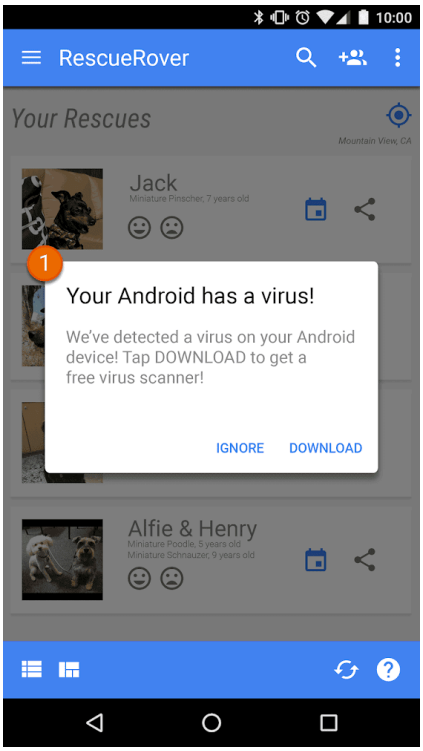
- Appar som renderar annonser som inte är synliga för användaren.
- Appar som automatiskt genererar klick på annonser utan användarens avsikt eller som skapar motsvarande nätverkstrafik i syfte att ge falska klick.
- Appar som skickar falska tillskrivningsklick för installationer i syfte att få betalt 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 annonspolicyn.

Social manipulering

Vi tillåter inte förfalskningar av appar där användaren luras att göra saker i tron att han eller hon använder den riktiga, betrodda appen.

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.

Payments

1. Utvecklare som tar betalt för appnedladdningar från Google Play måste använda Google Plays faktureringssystem som betalningsmetod för dessa transaktioner.
2. Appar som distribueras via Play och kräver eller accepterar betalning för åtkomst till funktioner eller tjänster i appen, inklusive appfunktioner, digitalt innehåll eller varor (sammantaget ”köp i appen”) måste använda Google Plays faktureringssystem för dessa transaktioner såvida inte avsnitt 3, avsnitt 8 eller avsnitt 9 gäller.

   Exempel på funktioner eller tjänster i appar som kräver användning av Google Plays faktureringssystem inbegriper men är inte begränsat till köp i appen av

   - objekt (till exempel virtuella valutor, extraliv, ytterligare speltid, tilläggsföremål, karaktärer och avatarer)
   - prenumerationstjänster (till exempel prenumerationer på innehåll i tränings-, spel-, dejting-, utbildnings-, musik- och videotjänster samt uppgraderingar av tjänster)

- funktioner eller innehåll i appar (till exempel den annonsfria versionen av en app eller nya funktioner som inte finns i gratisversionen)
- molnmjukvara och molntjänster (datalagringstjänster, produktivitetsmjukvara för företag och mjukvara för ekonomihantering).

3. Google Plays faktureringssystem får inte användas i följande fall:
   a. Om betalningen huvudsakligen avser något av följande:
      - Köp eller uthyrning av fysiska varor (till exempel matvaror, kläder, husgeråd och elektronik).
      - Köp av fysiska tjänster (till exempel transporttjänster, städtjänster, flygbiljetter, gymmedlemskap, hemkörning av mat, biljetter till liveevenemang).
      - Inbetalningar på en kreditkorts- eller hushållsräkning (t.ex. för tv- och telefontjänster).
   b. Betalningar inbegriper peer-to-peer-betalningar, onlineauktioner och donationer som undantas från skatt.
   c. Betalningen avser innehåll eller tjänster som förmedlar hasardspel online enligt beskrivningen i avsnittet Hasardspelsappar i policyn för hasardspel, spel och tävlingar om riktiga pengar.
   d. Betalningen avser en produktkategori som inte accepteras i enlighet med Googles innehållspolicy för betalningscentret .

      Obs! På vissa marknader erbjuder vi Google Pay för appar som säljer fysiska varor och/eller tjänster. Besök vår utvecklarsida för Google Pay om du vill veta mer.

4. Appar får inte leda användarna till en annan betalningsmetod än Google Plays faktureringssystem, med undantag för de villkor som beskrivs i avsnitt 3, avsnitt 8 och avsnitt 9. Detta förbud omfattar, men begränsas inte till, att leda användare till andra betalningsmetoder via
   - en apps information på Google Play
   - kampanjer i appar gällande köpbart innehåll
   - WebViews, knappar, länkar, meddelanden, annonser eller andra uppmaningar i appen
   - flöden i användargränssnittet i appen, inklusive flöden för att skapa konton eller registreringar, som hänvisar användare från en app till en annan betalningsmetod än Google Plays faktureringssystem i dessa flöden.
5. Virtuella valutor i appar får bara användas i den app eller det spel valutan köptes för.
6. Utvecklare måste tydligt och korrekt informera användarna om villkoren och priserna för deras appar eller funktioner i appar eller prenumerationer som de säljer. Priser i appar måste stämma överens med priserna som visas för användaren i faktureringsgränssnittet för Play. Om produktbeskrivningen på Google Play hänvisar till funktioner i appen som är avgiftsbelagda eller medför ytterligare avgifter måste det klart framgå i appinformationen att användarna måste betala för att använda dessa funktioner.
7. I appar och spel som innehåller funktioner för att få slumpmässigt utvalda virtuella objekt vid köp, inbegripet men inte begränsat till ”lootboxes”, måste oddsen för att få sådana objekt tydligt meddelas före och tidsmässigt nära köpet.
8. Om villkoren som beskrivs i avsnitt 3 inte är tillämpliga gäller följande: utvecklare av appar som distribueras via Play och som kräver eller accepterar betalning för åtkomst till köp i appen från användare i dessa länder/regioner får erbjuda användarna ett alternativt faktureringssystem utöver Google Plays faktureringssystem för dessa transaktioner om de fyller i deklarationsformuläret om fakturering för respektive program och godkänner de ytterligare villkor och programkrav som finns i formuläret.
9. Utvecklare av appar som distribueras på Play kan hänvisa användare i Europeiska ekonomiska samarbetsområdet (EES) ut ur appen, bland annat för att marknadsföra erbjudanden för digitala funktioner och tjänster i appen. Utvecklare som hänvisar användare i EES ut ur appen måste fylla i

deklarationsformuläret för programmet och godkänna alla ytterligare villkor och programkrav som finns i formuläret.

Obs! Du hittar tidsplaner och vanliga frågor om policyn i vårt hjälpcenter.

Annonser

I syfte att behålla en högklassig upplevelse tar vi annonsinnehåll, målgrupp, användarupplevelse, beteende samt säkerhet och integritet i beaktande. Vi betraktar annonser och tillhörande erbjudanden som en del av appen och de måste även följa alla andra policyer för Google Play. Vi har också ytterligare krav för annonser om du genererar intäkter från en app på Google Play som riktar sig mot barn.

Du kan läsa mer om våra policyer för appkampanjer och butiksuppgifter här, inklusive hur vi hanterar bedrägliga marknadsföringsmetoder.

Annonsinnehåll

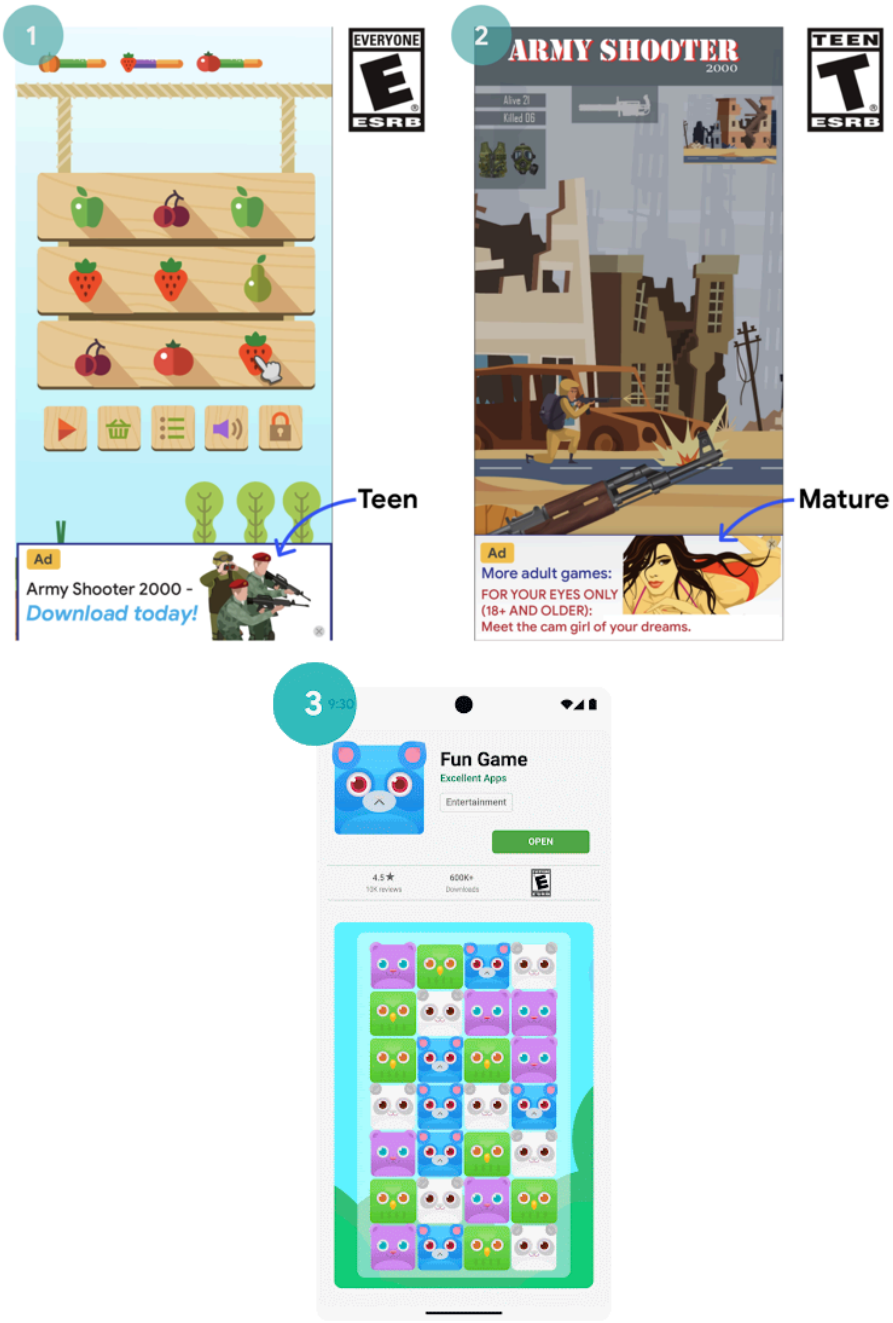
Annonserna och de tillhörande erbjudandena är en del av appen och måste följa vår policy för begränsat innehåll. Ytterligare krav gäller om appen är en app med hasardspel.

Olämpliga annonser

Annonserna och de erbjudanden som visas i appen (till exempel att annonsen förespråkar nedladdning av en annan app) måste vara lämpliga för appens innehållsklassificering , även om själva innehållet följer våra policyer.

Här är några exempel på vanliga överträdelser:

- Annonser som är olämpliga för appens innehållsklassificering



① Den här annonsen är olämplig (Tonåring) för appens innehållsklassificering (Alla)
② Den här annonsen är olämplig (Vuxen) för appens innehållsklassificering (Tonåring)
③ Annonserbjudandet (att ladda ned en app med innehållsklassificeringen Vuxen) är inte lämpligt för spelappen där annonsen visades på grund av spelappens innehållsklassificering (Alla)

Annonskrav för familjer

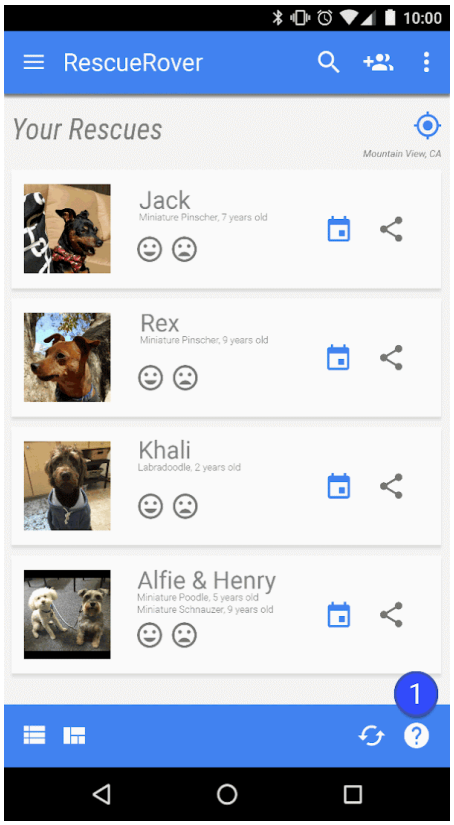
Om du får intäkter från en app på Google Play som riktar sig till barn är det viktigt att appen efterlever kraven i policyerna för familjeannonser och intäkter.

Vilseledande annonser

Annonser får inte efterlikna eller imitera en appfunktions användargränssnitt, till exempel aviseringar eller varningar i ett operativsystem. Det måste vara tydligt för användaren vilken app som visar varje annons.

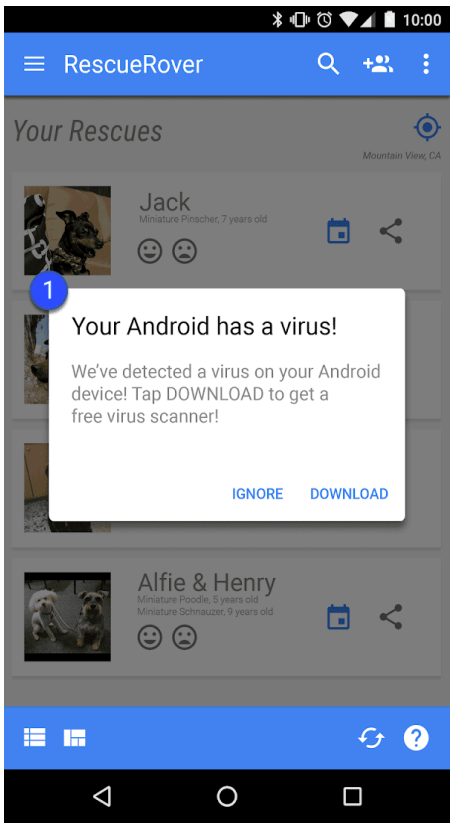
Här är några exempel på vanliga överträdelser:

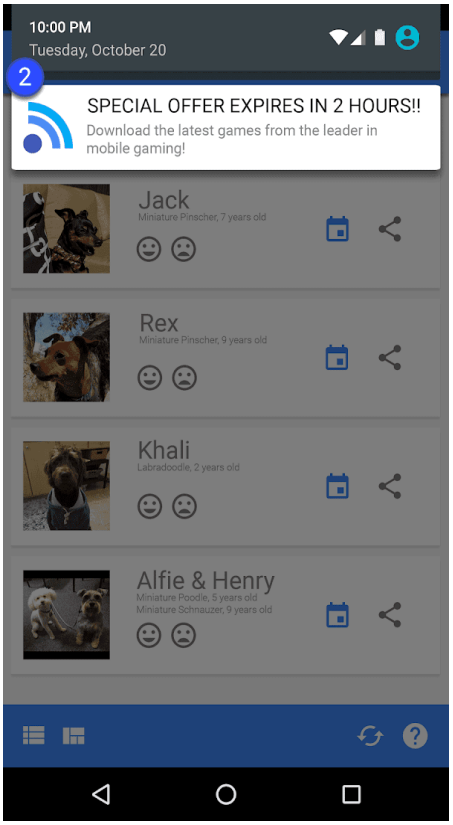
- Annonser som liknar användargränssnittet i en app:



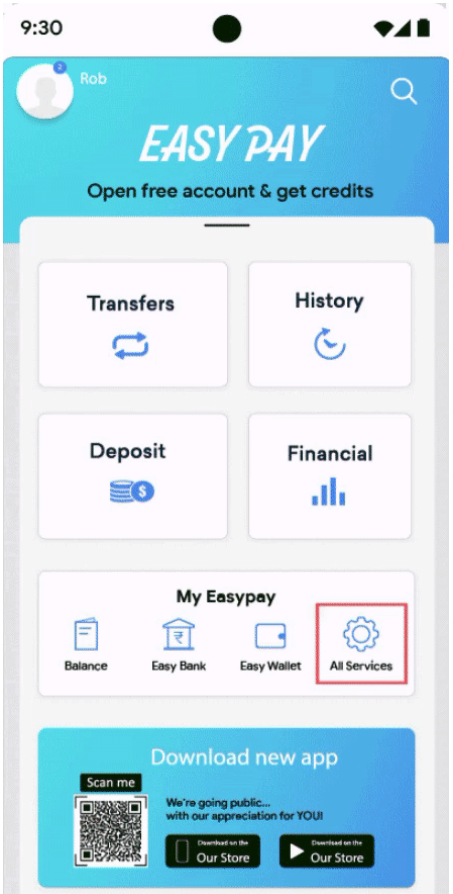
① Frågetecknet i den här appen är en annons som leder till en extern målsida.

- Annonser som liknar ett systemmeddelande:





① ② Exemplen ovan visar annonser som liknar olika systemmeddelanden.



① Exemplet ovan visar ett avsnitt med funktioner som imiterar andra funktioner men bara leder till annonser.

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.

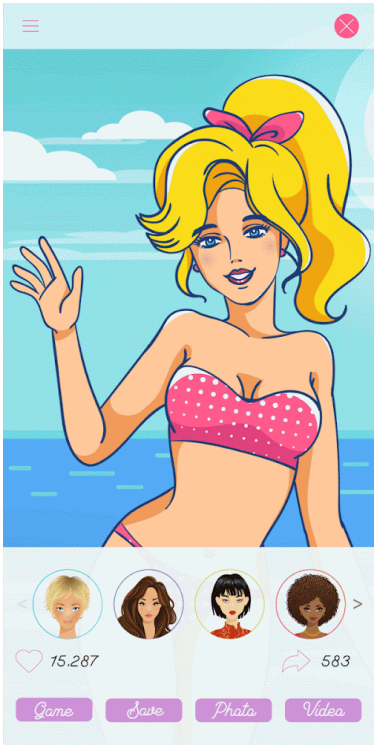
Appen får inte tvinga användare att klicka på annonser eller uppge personuppgifter i annonseringssyfte innan de kan använda appen till fullo. Annonser får bara visas i appen som de tillhör och får inte störa andra appar, annonser eller enhetens funktion, inklusive system- eller enhetsknappar och portar. Detta omfattar överlagringar, tillhörande funktioner och annonsenheter i form av widgetar. Om annonser som stör normal användning av appen visas måste de gå att stänga utan negativa konsekvenser.

Här är några exempel på vanliga överträdelser:

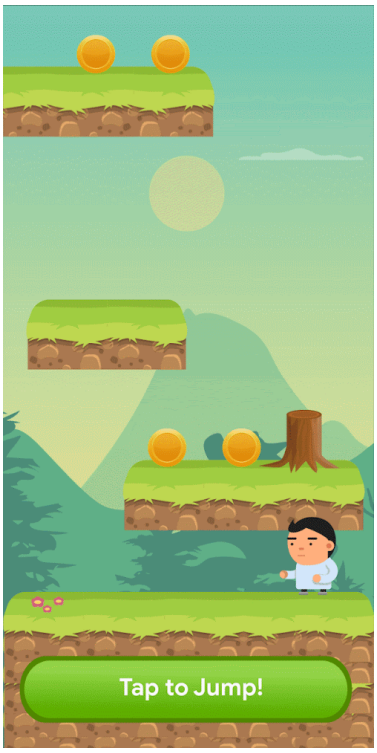
- Annonser som tar upp hela skärmen eller stör normal användning, och som inte har något tydligt sätt att stänga annonsen:

① Den här annonsen har ingen stängningsknapp.

- 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:

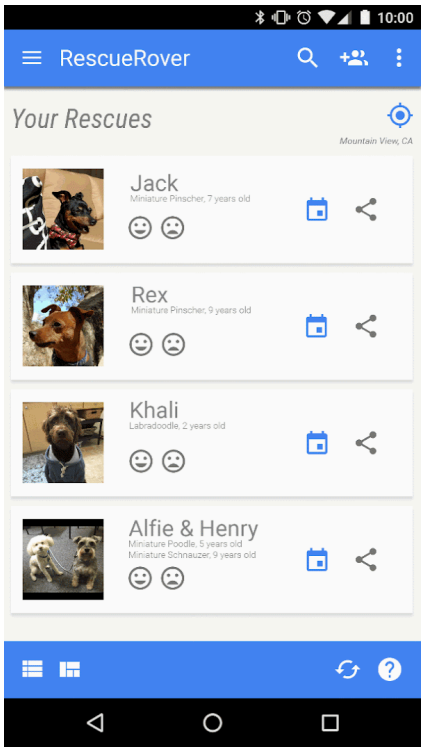


① Den här annonsen har en falsk stängningsknapp.



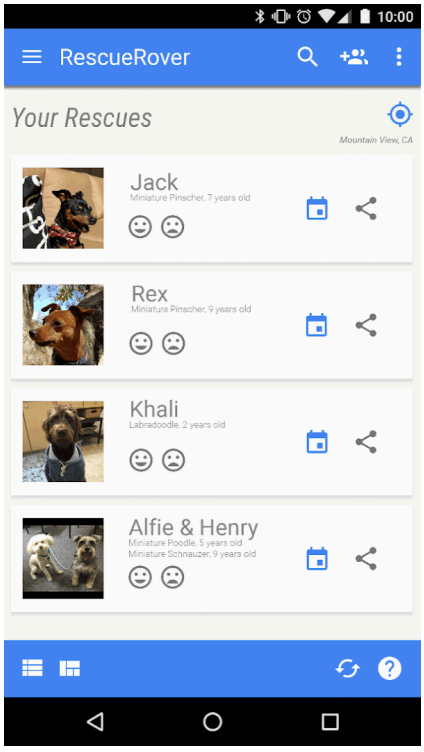
② Den här annonsen visas plötsligt i ett område där användaren är van vid att trycka på funktioner i appen.

- Annonser som visas utanför appen som de tillhör:



① Användaren navigerar till startskärmen från appen. Plötsligt visas en annons på startskärmen.

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



① Användaren försöker avsluta appen och navigera till startskärmen, men i stället avbryts det förväntade flödet av en annons.

Better Ads-upplevelser

Utvecklarna måste följa följande annonsriktlinjer för att användarna ska få en högklassig upplevelse när de använder appar från Google Play. Annonser får inte visas för användarna på följande oväntade sätt:

- Mellansidesannonser i alla format (video, GIF, statiska o.s.v.) som visas utan förvarning i helskärmsläge, vanligtvis när användaren har valt att göra något annat, är inte tillåtna.
  - Annonser som visas i början av en nivå i ett spel eller i början av ett innehållssegment i ett spel är inte tillåtna.
  - Mellansidesannonser med video i helskärmsläge som visas före en apps inläsningsskärm (välkomstskärmen) är inte tillåtna.
- Mellansidesannonser i alla format som visas i helskärmsläge och inte kan stängas efter 15 sekunder är inte tillåtna. Mellansidesannonser i helskärmsläge som visas när användaren valt att delta, eller mellansidesannonser i helskärmsläge som inte stör användarens åtgärder (till exempel efter poängskärmen i en spelapp) får visas i mer än 15 sekunder.

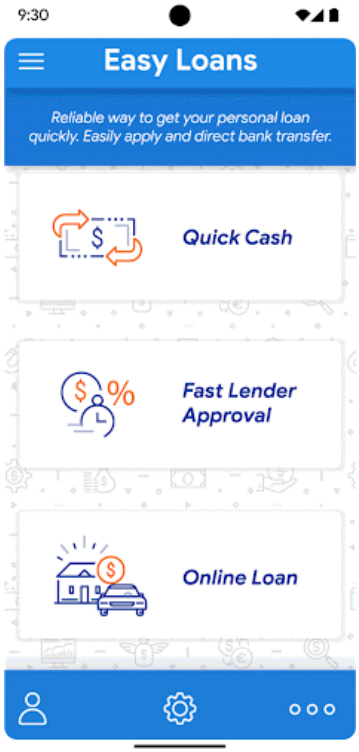
Den här policyn gäller inte premierade annonser som användarna uttryckligen valt att visa (till exempel en annons som utvecklarna uttryckligen erbjuder en användare att titta på i utbyte mot att låsa upp en viss funktion eller ett visst innehåll i ett spel). Policyn gäller inte heller intäktsgenerering och annonsering som inte stör den normala appanvändningen eller spelet (till exempel videoinnehåll med integrerade annonser eller bannerannonser som inte visas i helskärmsläge).

Dessa riktlinjer är inspirerade av riktlinjerna Better Ads Standards – Mobile Apps Experiences . Du kan läsa mer om Better Ads Standards på webbplatsen för Coalition for Better Ads .

Här är några exempel på vanliga överträdelser:

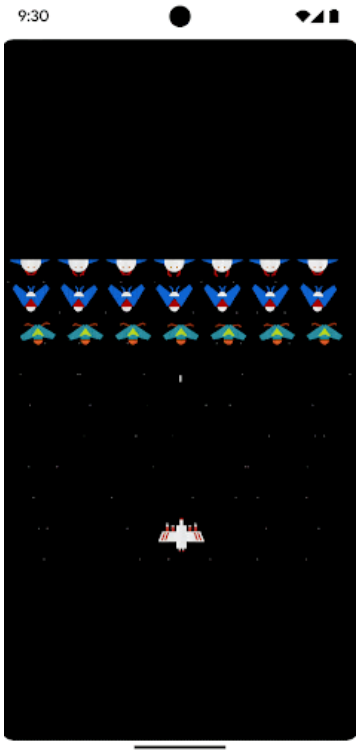
- Oväntade annonser som visas under spel eller i början av ett innehållssegment (till exempel efter att användaren har klickat på en knapp och innan den förväntade åtgärden inträffat). Dessa annonser räknas som oväntade för användaren eftersom denna snarare väntar sig att få börja spela eller interagera med ett visst innehåll.

① En oväntad statisk annons visas i början av en nivå i ett spel.



② En oväntad videoannons visas i början av ett innehållssegment.

- En helskärmsannons som visas under ett spel och inte kan stängas efter 15 sekunder.



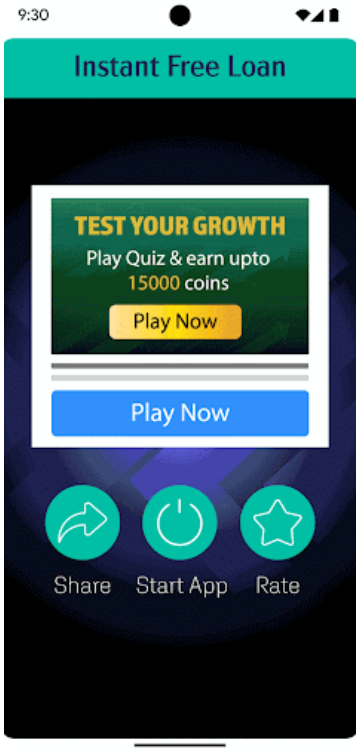
① En mellansidesannons visas under ett spel, men användaren får inte möjlighet att hoppa över annonsen inom 15 sekunder.

Made For-annonser

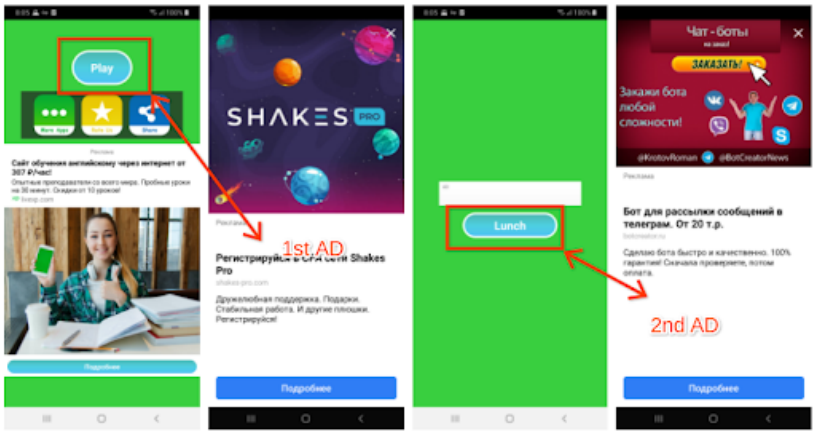
Vi tillåter inte appar som upprepade gånger visar mellansidesannonser för att distrahera användarna så att de inte kan interagera med en app och utföra uppgifter i appen.

Här är några exempel på vanliga överträdelser:

- Appar där en mellansidesannons placeras direkt efter en användaråtgärd (inbegripet men inte begränsat till klick, svepningar o.s.v.).



① Den första sidan i appen har flera knappar att interagera med. När användaren klickar på **Starta appen** för att använda appen visas en mellansidesannons. När annonsen har stängts återgår användaren till appen och klickar på **Tjänst** för att börja använda tjänsten, men en annan mellansidesannons visas.



② På den första sidan måste användaren klicka på **Spela** eftersom det är den enda knappen det går att klicka på för att använda appen. När användaren klickar på den visas en mellansidesannons. När annonsen har stängts klickar användaren på **Starta** eftersom det är den enda knappen han eller hon kan interagera med, och då visas en annan mellansidesannons.

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.

Annonsbedrägeri

Annonsbedrägeri är strängt förbjudet. Läs mer i vår policy för annonseringsbedrägeri.

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.

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 (AAID) 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 o.s.v.) 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 inte kopplas till uppgifter som kan kopplas till en specifik individ eller beständiga enhetsidentifierare (till exempel SSAID, MAC-adress, IMEI-kod o.s.v.) i något analyssyfte. I policyn om användaruppgifter finns ytterligare riktlinjer om beständiga enhetsidentifierare.
- **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 rätta dig efter det val som användaren har gjort för inställningen Välj bort intressebaserad annonsering eller Välj bort Personliga annonspreferenser. 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, konverteringsspårning, rapportering och säkerhet och bedrägeriupptäckt.
  - På nyare enheter tas identifieraren bort när användaren raderar Androids reklam-id. Alla som försöker komma åt identifieraren får en rad av nollor. En enhet utan reklam-id får inte kopplas till data som är länkad till eller härrör från ett tidigare reklam-id.
- **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 integritetsmeddelande. Läs mer om våra integritetsstandarder i vår policy om användardata .
- **Följa användarvillkoren**. Detta reklam-id får endast användas i enlighet med Google Plays programpolicy för utvecklare. 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.

Du hittar mer information i vår policy för användaruppgifter.

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. Vi tillåter inte appar där användarna utsätts för falska eller manipulativa köpupplevelser (inklusive köp i appar och prenumerationer).

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.

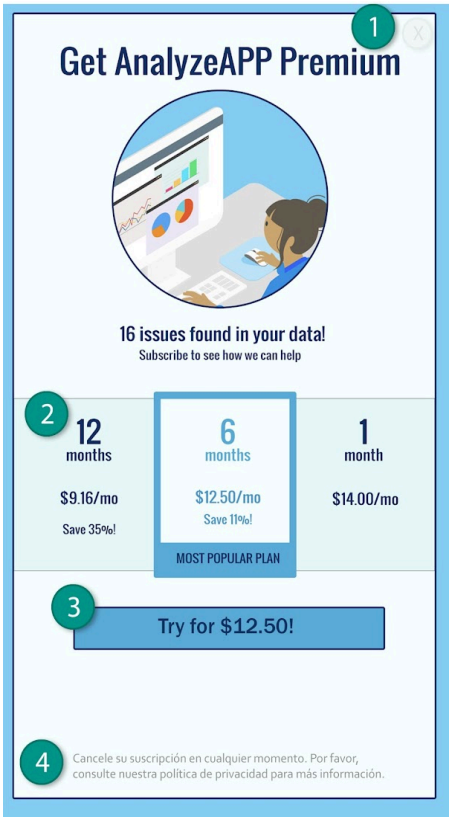
Prenumerationer måste ge användarna ett ihållande eller återkommande värde så länge de varar. De får inte uteslutande erbjuda användarna engångsförmåner (till exempel SKU:er som ger ett engångstillskott av saldo/pengar i appen eller spelboosters som bara går att använda en gång). Du får erbjuda incitament och kampanjbonusar, men det måste vara utöver prenumerationens ihållande eller återkommande värde så länge den varar**.** Om du inte erbjuder ett ihållande eller återkommande värde i produkten måste du använda produkt i appar i stället för prenumerationsprodukt.

Du får inte maskera eller felaktigt framställa engångsförmåner som prenumerationer. Detta omfattar att ändra prenumerationen till ett engångserbjudande (till exempel genom att avsluta, utfasa eller minimera det återkommande värdet) efter att användaren har tecknat den.

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 Kostnadsfri provperiod eller Testa Premium-medlemskap utan kostnad i tre dagar för en prenumeration som förnyas automatiskt.
- Flera skärmar i köpflödet som leder till att användaren oavsiktligt klickar på prenumerationsknappen.
- Prenumerationer utan ihållande eller återkommande värde, till exempel att användaren får 1 000 juveler första månaden och sedan minskas förmånen till en juvel i månaden för resten av prenumerationstiden.
- Det krävs att användaren registrerar sig för en prenumeration som förnyas automatiskt för att få en engångsförmån, och att säga upp användarens prenumeration utan att han eller hon har begärt det efter köpet.

Exempel 1:



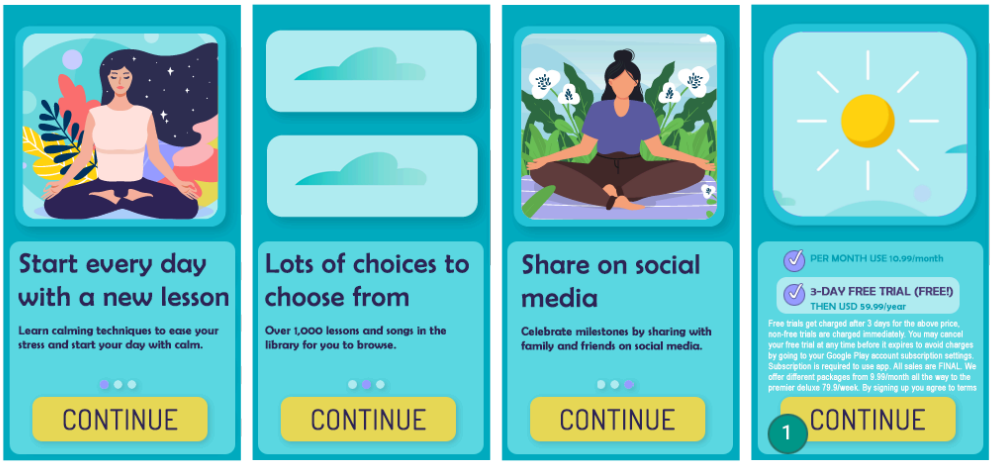
① Knappen Stäng syns inte tydligt och det kanske inte framgår för användarna att de får tillgång till funktionerna utan att tacka ja till prenumerationserbjudandet.

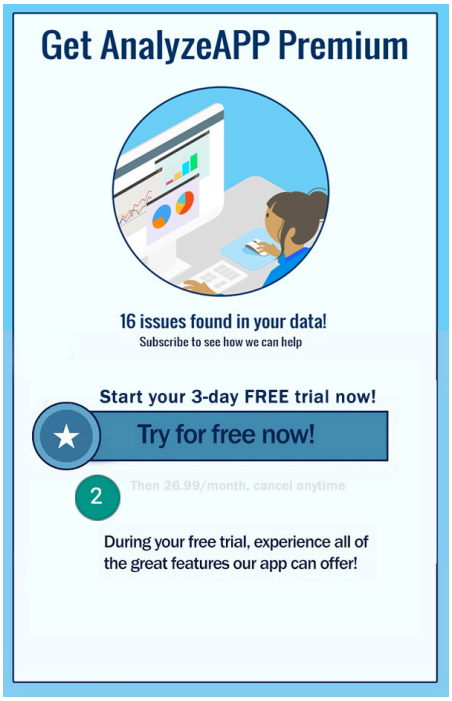
② Priset för erbjudandet visas bara per månad och det kanske inte framgår för användarna att de debiteras för sex månader i taget när de börjar prenumerera.

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.

Exempel 2:





① Användaren måste klicka flera gånger i samma knappområde så att hen oavsiktligt klickar på den sista Fortsätt-knappen för att prenumerera.

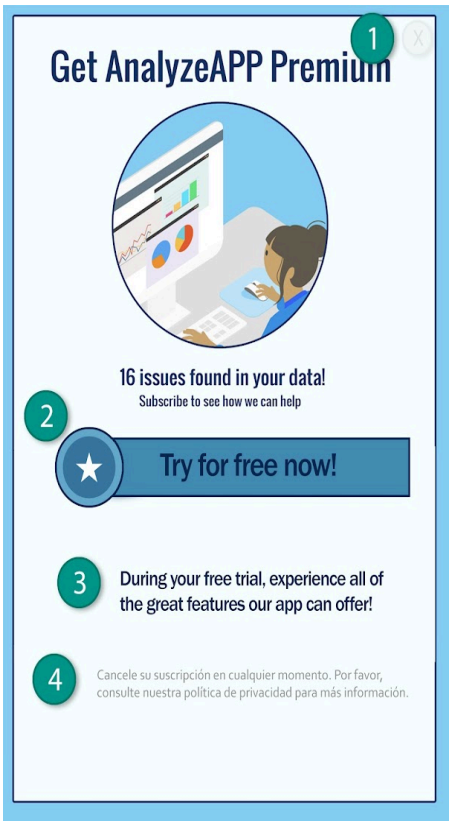
② Beloppet som användaren debiteras när provperioden löper ut är svårt att se, så användaren kanske tror att prenumerationen är kostnadsfri.

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, säga upp och återbetala prenumerationer

Om du säljer prenumerationer i appen/apparna måste du se till att den/de tydligt visar hur en användare kan hantera eller säga upp sin prenumeration. Du måste även inkludera åtkomst till en lättanvänd onlinemetod för att säga upp prenumerationen i appen. I appens kontoinställningar (eller motsvarande) kan du uppfylla kravet genom att inkludera

- en länk till prenumerationscentret för Google Play (för appar som använder Google Plays faktureringssystem) och/eller
- direkt åtkomst till uppsägningsprocessen.

Om en användare säger upp en prenumeration som köpts via Google Plays faktureringssystem är vår allmänna policy att användaren inte får en återbetalning för den innevarande faktureringsperioden. Användaren fortsätter i stället att få innehållet i prenumerationen under återstoden av den innevarande faktureringsperioden, oavsett vilket datum prenumerationen sades upp. Användarens uppsägning börjar gälla när den innevarande faktureringsperioden är slut.

Du (som innehålls- eller åtkomstleverantör) kan införa en mer flexibel återbetalningspolicy direkt för dina användare. Det är ditt ansvar att meddela användarna om eventuella ändringar i din prenumerations-, uppsägnings- eller återbetalningspolicy och att se till att de följer gällande lag.

Programmet för självcertifierade annons-SDK:er för familjer

Om du visar annonser i appen och endast barn ingår i målgruppen i enlighet med familjepolicyn måste du använda annons-SDK:er som har självcertifierat att de efterlever Google Plays policyer, inklusive kraven för självcertifierade annons-SDK:er för familjer nedan.

Om både barn och äldre användare ingår i målgruppen för appen måste du säkerställa att alla annonser som visas för barn endast kommer från någon av dessa versioner av självcertifierade annons-SDK (till exempel genom att använda skärmar för ålderskontroll).

Observera att det är ditt ansvar att se till att alla SDK-versioner du implementerar i appen, inklusive självcertifierade annons-SDK:er, följer alla gällande policyer samt lokala lagar och regler. Google ger inga löften eller garantier om att informationen som annons-SDK:erna tillhandahåller vid självcertifieringen är korrekt.

Du måste bara använda självcertifierade annons-SDK:er för familjer om du använder annons-SDK:er för att visa annonser för barn. 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 Google Plays policy för användaruppgifter och familjepolicy :

- intern annonsering där SDK:er används för hantering av korsmarknadsföring av dina appar eller annan media och andra produkter du säljer
- att ingå direktavtal med annonsörer där SDK:er används för hantering av annonsutrymme.

Krav för självcertifierade annons-SDK:er för familjeprogram

- Definiera vad som utgör olämpligt innehåll och beteende i annonser och förbjud det i villkoren eller policyn för annons-SDK:et. Definitionerna ska följa Google 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 Google 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 genom att skicka in en testapp och de uppgifter som anges i intresseanmälan nedan, för att Google ska kunna verifiera att annons-SDK:et efterlever alla självcertifieringskrav. Svara inom rimlig tid på eventuella efterföljande förfrågningar om information, till exempel genom att skicka in en ny version för att verifiera att versionen av annons-SDK:et följer alla självcerifieringskrav.
- Självcertifiera att alla nya versioner följer Google Plays senaste programpolicy för utvecklare, inklusive kraven i familjepolicyn.

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

Mer information om att vattenstämpla annonsmaterial och tillhandahålla en testapp finns här .

Här hittar du förmedlingskrav för annonsvisningsplattformar gällande annonser som visas för barn:

- Använd endast självcertifierade annons-SDK:er för familjer 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 för familjer, och de kan kontrollera vilka specifika versioner av annons-SDK:erna som är självcertifierade för användning i appar avsedda för familjer.

Utvecklare kan även dela detta formulär för intresseanmälan med leverantörer av annons-SDK:er som vill implementera självcertifiering.

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 (t.ex. annonser) som är vilseledande eller skadliga för användare eller utvecklare. Marknadsföringsmetoder vars beteende eller innehåll bryter mot vår programpolicy för utvecklare anses vara vilseledande eller skadliga.

Här är några exempel på vanliga överträdelser:

- Användning av vilseledande annonser på webbplatser, i appar eller andra egendomar, till exempel aviseringar som liknar systemmeddelanden och varningar.
- Användning av sexuellt explicita annonser för att omdirigera användare till appens butiksuppgifter på Google Play för nedladdning.
- Marknadsföring eller installationsstrategier som omdirigerar användare till Google Play eller laddar ned appar utan att användaren kan göra ett välinformerat val om det.
- Oönskad marknadsföring via sms-tjänster.
- Text eller bild i appens titel, ikon eller utvecklarens namn som anger butiksrankning eller -resultat, pris- eller marknadsföringsinformation eller antyder en koppling till befintliga Google Play-program.

Du ansvarar för att se till att alla annonsnätverk, närstående bolag och annonser som är kopplade till appen efterlever dessa policyer.

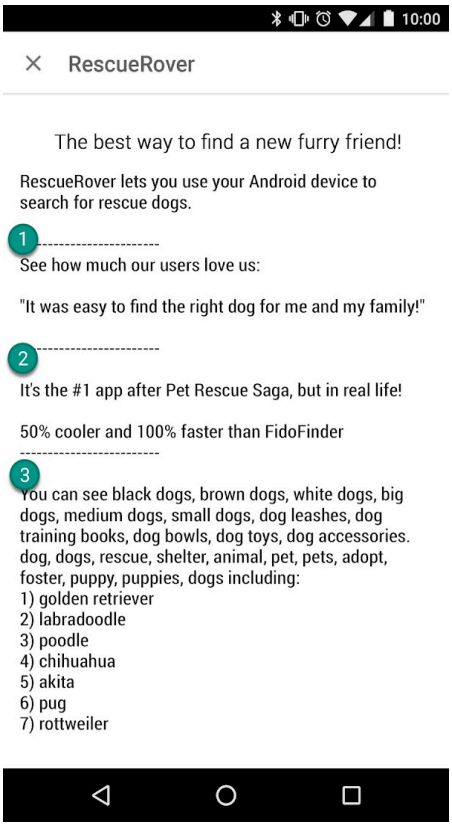
Metadata

Användare läser beskrivningarna av din app för att förstå dess funktioner och syfte. Vi tillåter inte appar med vilseledande, felaktigt formaterad, otydlig, irrelevant, överflödig eller olämplig metadata. Det gäller bland annat appbeskrivningen, utvecklarens namn, appens namn, ikon, skärmbilder och kampanjbilder. Utvecklare måste tillhandahålla en tydlig och välskriven beskrivning av appen. Vi tillåter heller inte användarrekommendationer som inte tillskrivs någon eller som är anonyma i appens beskrivning.

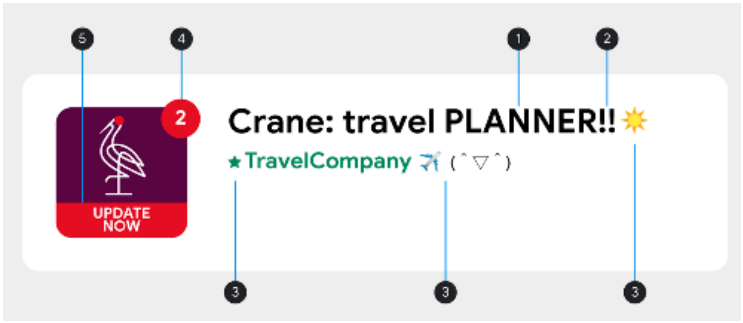
Många användare hittar och tar reda på mer om din app utifrån appens titel, ikonen och utvecklarnamnet. Använd inte emojis, uttryckssymboler eller flera specialtecken i dessa metadataelement. Undvik att bara använda VERSALER om inte varumärkesnamnet skrivs så. Vi tillåter inte vilseledande symboler i appikoner, till exempel: punktindikator för nya meddelanden när det inte finns några och symboler för att ladda ned/installera om innehållet som laddas ned inte är kopplat till appen. Appens titel får vara högst 30 tecken. Använd inte text eller en bild i appens titel, ikon eller utvecklarens namn som anger butiksrankning eller -resultat, pris- eller marknadsföringsinformation eller antyder en koppling till befintliga Google Play-program.

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

Här är några exempel på vanliga överträdelser:

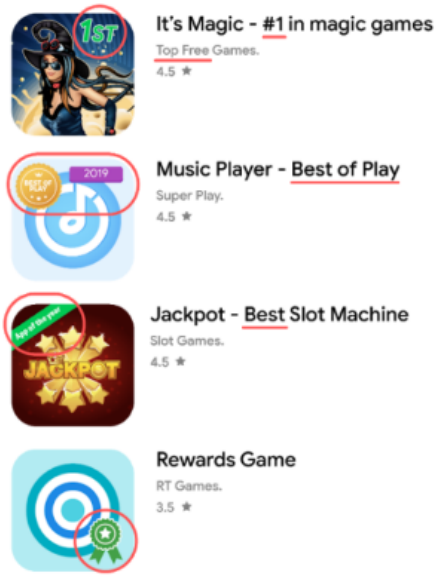


① Anonyma användarrekommendationer
② Jämförelser av uppgifter mellan appar och varumärken
③ Väggar av text eller horisontala eller vertikala listor av ord

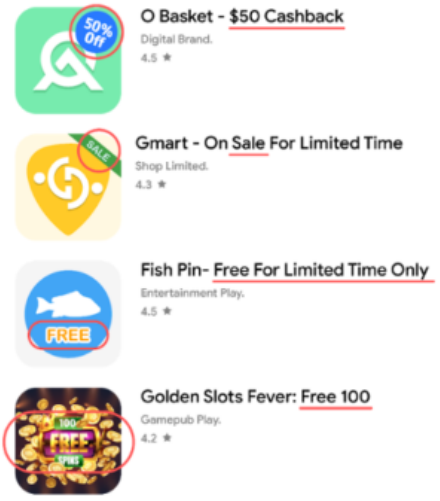


① Skriva hela ord i VERSALER förutom i varumärkesnamn
② Flera specialtecken i följd som inte är relevanta för appen
③ Använda emojis, uttryckssymboler (inklusive kaomojis) och specialtecken
④ Vilseledande symboler
⑤ Vilseledande text

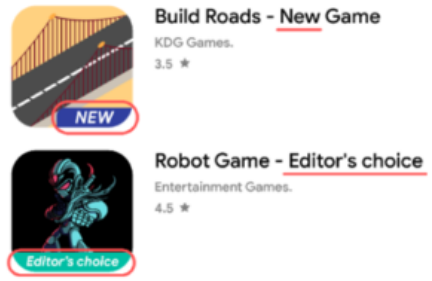
- Bilder eller text som anger butiksrankning eller -resultat, till exempel Årets app, Nr. 1, Det bästa på Play 20XX, Populär, ikoner för utmärkelser osv.



- Bilder eller text som anger pris och kampanjuppgifter, till exempel 10 % rabatt, 50 USD tillbaka, Gratis under en begränsad tid osv.



- Bilder eller text som anger Google Play-program, till exempel Redaktionens val, Nyhet osv.



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:

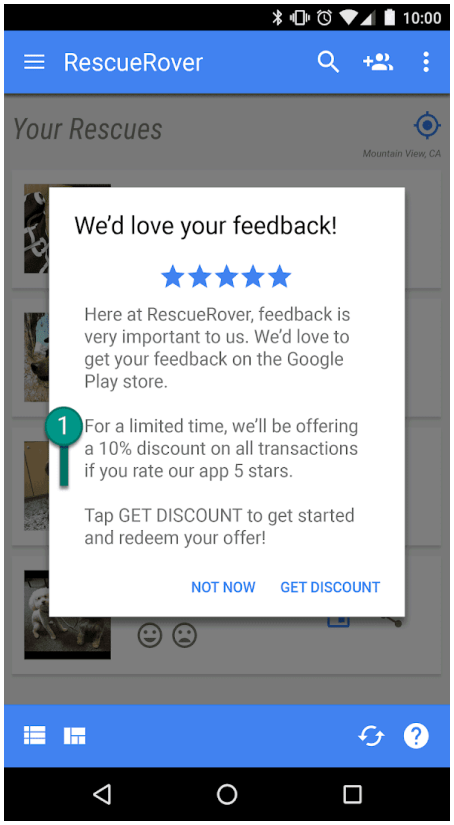
- Betona vad som är bra med din app. Dela intressanta och spännande fakta så att användarna förstår vad som gör appen speciell.
- Försäkra dig om att appens titel och beskrivning beskriver appens funktioner på ett korrekt sätt.
- Undvik upprepade eller irrelevanta sökord eller hänvisningar.
- Skriv en 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 på Google Play. Detta omfattar, men är inte begränsat till, att höja produktbetyg, recensioner eller antal installationer på otillåtna sätt, såsom att erbjuda ersättning för eller skicka bedrägliga recensioner och betyg eller att ha som grundfunktion i appen att erbjuda användare ersättning för att installera andra appar.

Här är några exempel på vanliga överträdelser:

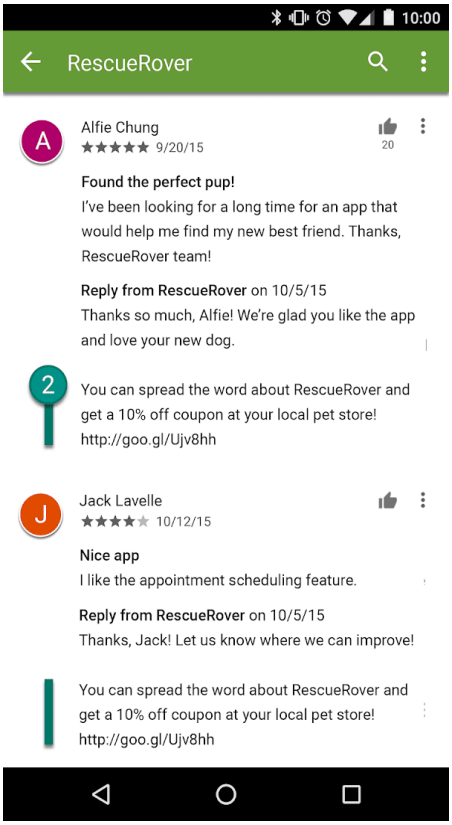
- Be användarna att betygsätta din app och erbjuda ersättning:



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

- Låtsas vara en legitim användare för att upprepade gånger betygsätta appen för att påverka placeringen 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.

Innehållsklassificeringar

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. Appar utan innehållsklassificering tas bort från Play Butik.

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

En nyhetsapp är en app som

- betecknats som nyhetsapp på Google Play Console
- listas i kategorin Nyheter och tidskrifter i Google Play Butik och beskrivs som nyheter i appens titel, ikon, utvecklarnamn eller beskrivning.

Exempel på appar i kategorin Nyheter och tidskrifter som räknas som nyhetsappar:

- Appar som betecknas som nyheter i appens beskrivning, inklusive men inte begränsat till:
  - senaste nytt
  - tidning
  - senaste nyheter
  - lokala nyheter
  - dagsnyheter
- appar som innehåller ordet ”nyheter” i titel, ikoner eller utvecklarnamn.

Om en app i första hand innehåller användargenererat innehåll (t.ex. appar för sociala medier) ska de dock inte anges som nyhetsappar, och anses heller inte vara nyhetsappar.

Nyhetsappar som kräver att en användare köper ett medlemskap måste ge användarna möjlighet att förhandsgranska innehållet i appen före köpet.

Nyhetsappar måste

- informera om apputgivaren och källorna till nyhetsartiklarna, inklusive men inte begränsat till ursprunglig utgivare eller författare för varje artikel. I de fall då det inte är brukligt att ange enskilda artikelförfattare måste nyhetsappen själv vara ursprunglig artikelutgivare. Observera att länkar till konton i sociala medier inte är tillräckliga uppgifter om författare eller utgivare.
- ha en webbsida eller sida i appen som är till för kontaktuppgifter och tydligt märkt som sådan, är lätt att hitta (t.ex. med en länk längst ned på startsidan eller i navigeringsfältet) och innehåller giltiga kontaktuppgifter till nyhetsutgivaren med antingen en e-postadress eller ett telefonnummer för kontakt. Observera att länkar till konton i sociala medier inte är tillräckliga kontaktuppgifter för utgivare.

Nyhetsappar får inte

- innehålla markanta stavfel och/eller grammatiska fel
- enbart ha statiskt innehåll (t.ex. innehåll som är över tre månader gammalt)
- ha affiliate-marknadsföring eller annonsintäkter som primärt syfte.

Observera att annonser och annan marknadsföring *får* användas för intäktsgenerering i nyhetsappar så länge appens huvudsakliga syfte inte är att sälja produkter eller tjänster eller att generera intäkter från annonser.

Nyhetsappar som sammanställer nyheter från olika nyhetskällor måste tydligt ange innehållets publiceringskälla i appen och alla källor måste uppfylla kraven i nyhetspolicyn.

Läs mer om hur du bäst anger informationen som krävs i den här artikeln .

Spam, funktioner och användarupplevelse

Appar måste uppfylla grundläggande krav på funktion och innehåll för en engagerande användarupplevelse. 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.

Här är ett exempel på en vanlig överträdelse:

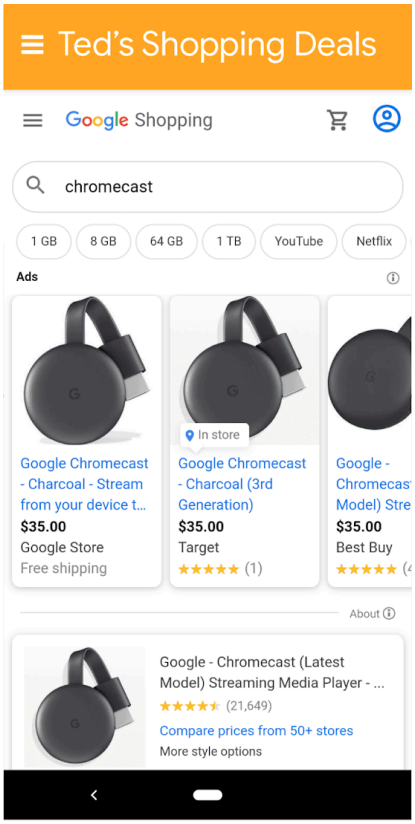
- När användaren trycker på knappen Dela skickar appen meddelanden för användarens räkning utan att användaren kan bekräfta innehållet eller de avsedda mottagarna:

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:



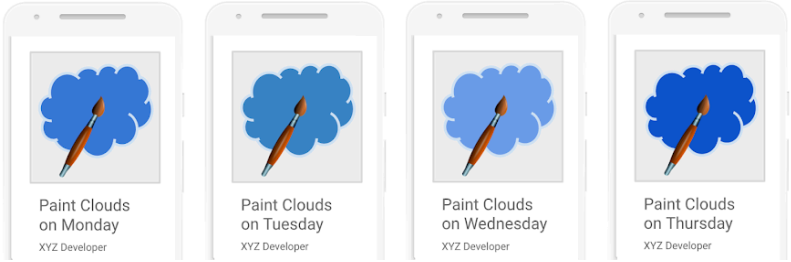
① Denna app heter Ted's Shopping Deals och den tillhandahåller endast en visning av Google Shopping.

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.



Funktioner, innehåll och användarupplevelse

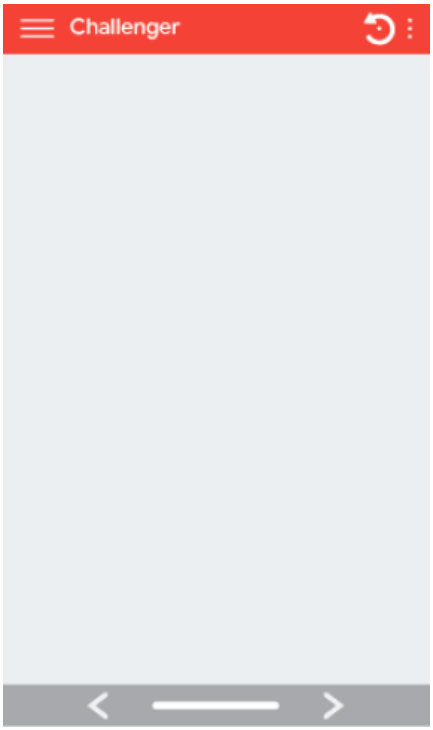
Appar bör tillhandahålla en stabil, responsiv och engagerande användarupplevese. Appar som kraschar, som inte fungerar som appar bör fungera, inte har engagerande innehåll eller som uppvisar annat beteende som inte är förenligt med en fungerande och engagerande användarupplevelse är inte tillåtna på Google Play.

Begränsade funktioner och begränsat innehåll

Vi tillåter inte appar som endast har begränsade funktioner och begränsat innehåll.

Här är ett exempel på en vanlig överträdelse:

- Appar som är statiska utan appspecifika funktioner, till exempel appar för endast text eller PDF-filer
- Appar med väldigt lite innehåll och som inte tillhandahåller en engagerande användarupplevelse, till exempel appar med en enda bakgrund
- Appar som inte har utformats för att göra något eller fylla någon funktion



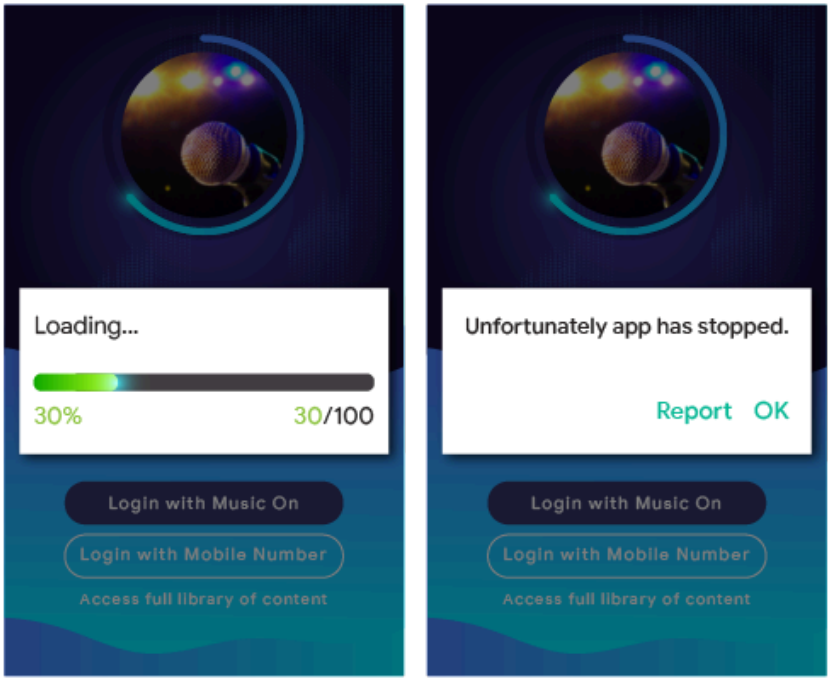
Defekt funktion

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

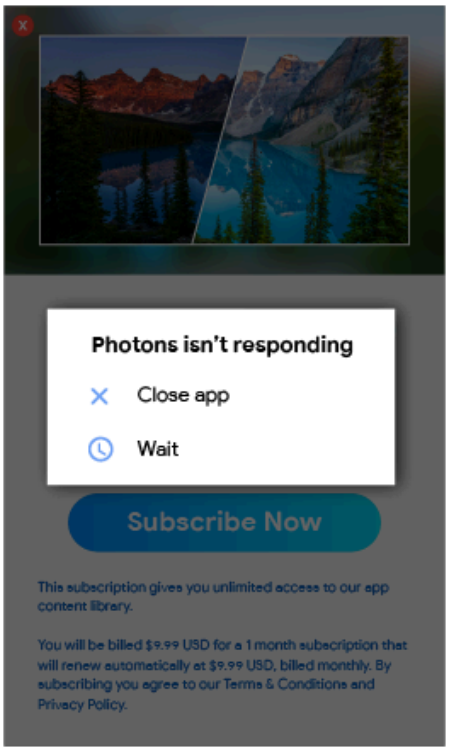
Här är några exempel på vanliga överträdelser:

- 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 snabbappar eller installerade appar 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 installationsuppmaningar i snabbappen.
- Inte presentera installationsuppmaningen 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 och (2) inte kan återställas av användaren. Några exempel är

- 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 av användare med hjälp av dessa identifierare eller andra metoder.

Nätverkstrafik

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

Policyn om emojis på Android

Vi har utformat vår policy om emojis för att uppmuntra till en inkluderande och konsekvent användarupplevelse. Därför måste alla appar ha stöd för den senaste versionen av Unicode-emojis när de körs på Android 12 eller senare.

Appar som använder standardemojis på Android utan anpassade implementeringar använder redan den senaste versionen av Unicode-emojis när de körs på Android 12 eller senare.

Appar med anpassade emojiimplementeringar, inklusive sådana som tillhandahålls via bibliotek från tredje part, måste ha fullt stöd för den senaste Unicode-versionen inom fyra månader efter att nya versioner av Unicode-emojis blivit tillgängliga när de körs på Android 12 eller senare.

I den här guiden kan du läsa mer om hur du stödjer moderna emojis.

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.

Google Plays familjepolicyer

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.

Alla appar som följer Google Plays familjepolicyer kan välja att bli granskade för programmet Godkänd av lärare, men vi kan inte garantera att appen blir godkänd för programmet.

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.

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. Om appen har innehåll som inte är lämpligt globalt, men där innehållet anses vara lämpligt för minderåriga användare i en viss region, kan appen vara tillgänglig i den regionen (regionsbegränsning) men inte i andra regioner.
2. **Appens funktioner:** Appen får inte enbart innehålla en WebView av en webbplats eller ha som primärt syfte att dirigera trafik till en webbplats utan tillstånd från webbplatsägaren eller administratören.
3. **Svar i Google Play Console:** Du måste ge korrekta svar på frågor om appen i Play Console och uppdatera svaren så att de överensstämmer med eventuella ändringar av appen. I detta ingår, men är inte begränsat till, att tillhandahålla korrekta svar om appen i avsnittet Målgrupp och innehåll, avsnittet om datasäkerhet och formuläret för IARC:s innehållsklassificering.
4. **Datahantering:** 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 och data om annonsanvändning. Du måste även säkerställa att appen efterlever datahanteringen nedan:
   - Appar som endast riktar sig till barn får inte överföra Androids reklam-id (AAID), serienummer för SIM-kort, serienummer för version, BSSID, MAC, SSID, IMEI-koder och/eller IMSI.
     - Appar som endast riktar sig till barn ska inte begära behörigheten AD_ID när de är inriktade på Android API 33 eller senare.
   - Appar som riktar sig till både barn och äldre målgrupper får inte överföra AAID, serienummer för SIM-kort, versionens serienummer, BSSID, MAC, SSID, IMEI-kod och/eller IMSI-nummer från barn eller användare i okänd ålder.
   - TelephonyManager i Android API får inte begära enhetens telefonnummer.

- Appar som är inriktade enbart på barn får inte begära platsbehörighet eller samla in, använda eller överföra exakt plats.
- 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.

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 främst riktar sig till barn.
     - Det gäller till exempel en API-tjänst som använder OAuth-teknik för autentisering och auktorisering vars användarvillkor anger att den inte är godkänd för användning i tjänster som riktar sig mot barn.
   - Implementera inte API:er eller 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. Appar som riktar sig till både barn och äldre målgrupper får inte kräva att användarna använder appinnehåll via API:er eller SDK:er som inte är godkända för tjänster som riktar sig till barn.

6. **Förstärkt verklighet (AR):** 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 (var till exempel uppmärksam på omgivningen).
   - Användning av enheter som inte är lämpliga för barn (till exempel Daydream och Oculus) får inte krävas för appen.

7. **Sociala appar och funktioner:** Om användare kan dela eller utbyta information i appen måste du uppge korrekta uppgifter om funktionerna i frågeformuläret för innehållsklassificering i Play Console.
   - Sociala appar: En social app är en app vars huvudsyfte är att göra det möjligt för användarna att dela innehåll i fritt format och kommunicera med stora grupper människor. Alla sociala appar som riktar sig till en målgrupp där barn ingår måste visa en påminnelse i appen om säkerhet på nätet och att vara medveten om riskerna som interaktioner online kan innebära i den verkliga världen innan barn kan utbyta information eller innehåll i fritt format. En vuxen måste även vidta åtgärder innan barn kan utbyta personliga uppgifter.
   - Sociala funktioner: En social funktion är tilläggsfunktioner i appen som gör det möjligt för användarna att dela innehåll i fritt format eller kommunicera med stora grupper människor. Alla appar som riktar sig till en målgrupp där barn ingår och innehåller sociala funktioner måste visa en påminnelse i appen om säkerhet på nätet och att vara medveten om riskerna som interaktioner online kan innebära i den verkliga världen innan barn kan utbyta information eller innehåll i fritt format. Det måste även finnas ett sätt för vuxna att hantera sociala funktioner för barn, inbegripet men inte begränsat till att aktivera/inaktivera den sociala funktionen eller ställa in funktionen på olika nivåer. Slutligen måste en vuxen även vidta åtgärder innan barn kan utbyta personliga uppgifter.
   - Med att en vuxen måste vidta åtgärder menas att det finns en mekanism för att verifiera att användaren inte är ett barn, och att barn inte kan ange fel ålder för att få åtkomst till delar av appen som är avsedda för vuxna (d.v.s. pinkod för vuxna, lösenord, födelsedatum, verifiering via e-post, fotolegitimation, kreditkort eller personnummer).
   - Sociala appar vars huvudsyfte är att chatta med andra man inte känner får inte rikta sig till barn. Exempel: appar där man chattar med slumpmässigt utvalda människor, dejtingappar, öppna chattrum för barn, osv.

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-lagen Allmänna dataskyddsförordningen (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 strider mot Google Plays programpolicy för utvecklare .
- Appar som visar barnförbjudna annonser (t.ex. våldsamt innehåll, sexuellt innehåll, hasardspelsinnehåll) för barn.

Annonser och intäkter

Om du får intäkter från en app som riktar sig till barn på Play är det viktigt att appen efterlever följande krav i policyerna för familjeannonser och intäkter.

Policyerna nedan gäller för all annonsering och intäktsgenerering i appen, inklusive annonser, korsmarknadsföring (t.ex. för dina appar och appar från tredje part), erbjudanden om köp i appen och allt övrigt kommersiellt innehåll (t.ex. betald produktplacering). All annonsering och intäktsgenerering 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.

Annonskrav

Om annonser visas för barn eller användare i okänd ålder i appen måste du göra följande:

- endast använda Google Plays program för självcertifierade annons-SDK:er för att visa annonser 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 tillämpliga branschstandarder för annonsering som riktar sig till barn efterlevs.

Krav på annonsformat

Du får inte visa annonser eller generera intäkter i appen med hjälp av vilseledande innehåll och de får inte vara utformade på ett sätt som leder till oönskade klick av minderåriga användare.

Följande är förbjudet om barn är den enda målgruppen för appen. Om appen är riktad till både barn och äldre målgrupper är följande förbjudet när annonser visas för barn eller användare i okänd ålder:

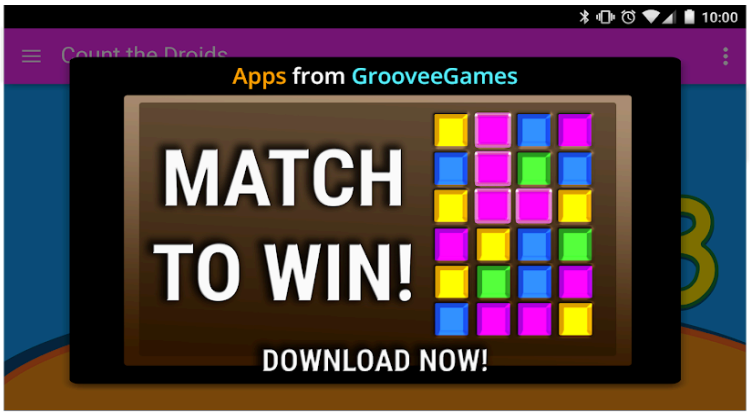
- störande intäktsgenerering och annonsering, inklusive sådan som tar upp hela skärmen eller stör normal användning och som inte har något tydligt sätt att stänga annonsen (t.ex. annonsväggar)

- intäktsgenerering och annonsering som stör normal användning av appar eller spel, inklusive premierade annonser eller annonser med medgivande, som inte går att stänga efter fem sekunder
- (intäktsgenerering och annonsering som inte stör normal användning av appar eller spel kan visas i mer än fem sekunder, t.ex. videoinnehåll med integrerade annonser)
- intäktsgenerering och annonsering med mellansidesannonser som 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)
- intäktsgenerering och annonsering som inte tydligt går att skilja från appinnehållet, som offerwalls och andra helskärmsannonsupplevelser
- att manipulera användare till att titta på annonser eller göra köp i appen med hjälp av känslomässig utpressning eller stötande innehåll
- vilseledande annonser som tvingar användaren att klicka på dem genom att använda en stängningsknapp som utlöser en till annons, eller genom att annonserna plötsligt visas i delar av appen där användaren oftast trycker på en annan funktion
- att inte göra skillnad på köp i appen som görs med virtuella pengar i spelet och köp med riktiga pengar.

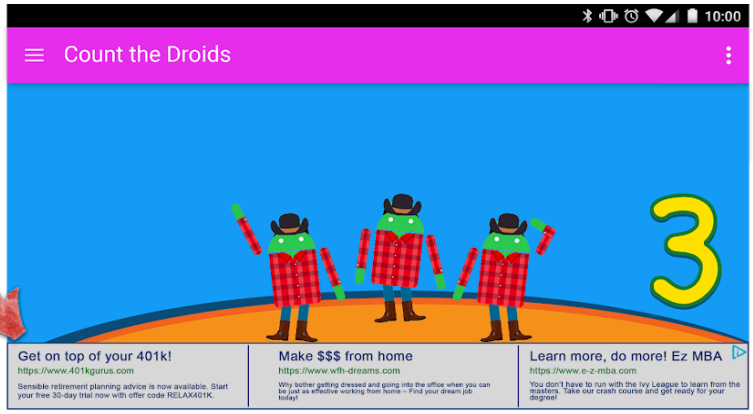
Här är några exempel på vanliga överträdelser:

- Annonser och intäktsgenerering som flyttas undan användarens finger när användaren försöker att stänga dem.
- Annonser och intäktsgenerering med erbjudanden som inte går att stänga efter fem (5) sekunder, så som visas i exemplet nedan:

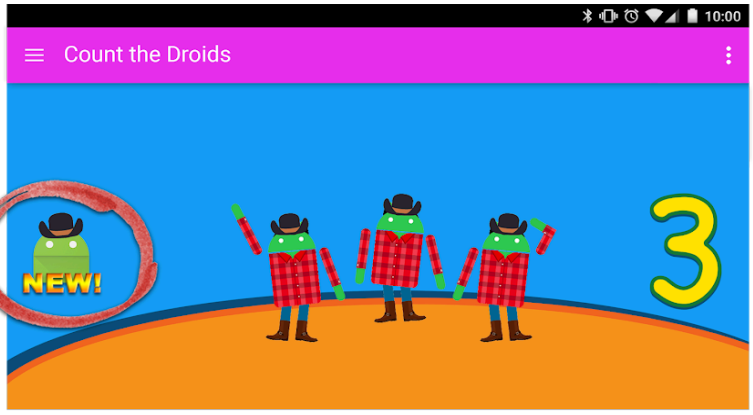
- Annonser och intäktsgenerering som tar upp stora delar av skärmen utan att användaren på ett enkelt sätt kan stänga dem, så som visas i exemplet nedan:



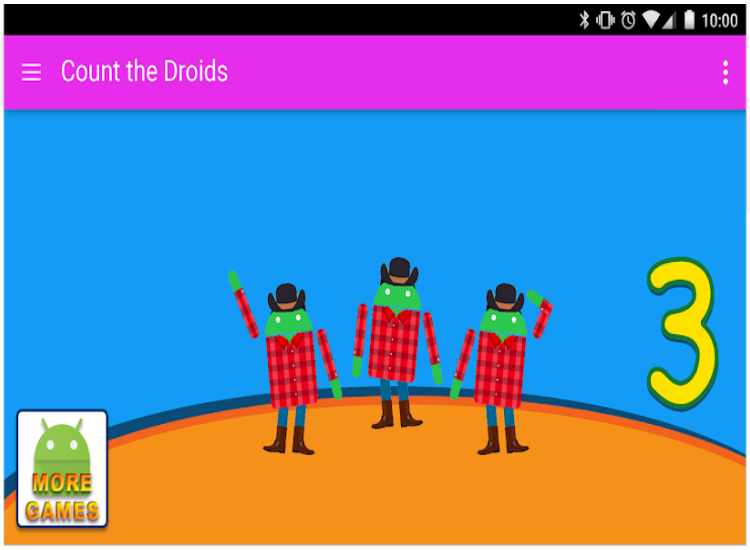
- Bannerannonser som visar flera erbjudanden, så som visas i exemplet nedan:



- Annonser och intäktsgenerering som användaren kan förväxla med innehåll i appen, så som visas i exemplet nedan:



- Marknadsföring för dina andra butiksuppgifter i Google Play med hjälp av knappar, annonser eller annan intäktsgenerering 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.
- **Barnförbjudet eller sexuellt provokativt innehåll**: Annonser med sexuellt, provokativt eller barnförbjudet 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.

Annons-SDK:er

Om du visar annonser i appen och endast barn ingår i målgruppen måste du använda enbart versioner av självcertifierade annons-SDK:er för familjer . 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 versioner av Google Plays självcertifierade annons-SDK:er.

Läs policysidan för programmet för självcertifierade annons-SDK:er för familjer om du vill veta mer om dessa krav, och här kan du se en aktuell lista över versioner av självcertifierade annons-SDK:er för familjer.

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.

Policy för självcertifierade annons-SDK:er för familjer

Det är viktigt för oss på Google Play att barn och familjer får en säker upplevelse. En stor del i detta är att se till att alla annonser som visas för barn är lämpliga för deras ålder och att deras data hanteras på ett lämpligt sätt. För att uppnå det här målet kräver vi att annons-SDK:er och förmedlingsplattformar självcertifierar att de är lämpliga för barn och efterlever Google Plays

programpolicyer för utvecklare och Google Plays familjepolicyer, inklusive kraven för programmet för självcertifierade annons-SDK:er för familjer.

Programmet för självcertifierade annons-SDK:er för familjer är ett viktigt verktyg för utvecklare att identifiera vilka annons-SDK:er eller förmedlingsplattformar som har självcertifierat att de är lämpliga att använda i appar som särskilt riktar sig till barn.

Felaktig framställning av någon information om ditt SDK, inklusive i intresseformuläret, kan leda till att SDK:et tas bort eller stängs av från programmet för självcertifierade annons-SDK:er för familjer. Därför är det viktigt att uppgifterna är korrekta.

Policykrav

Om du har ett SDK eller en medlingsplattform som används i appar som ingår i Google Plays program för familjer måste du följa alla utvecklarpolicyer för Google Play, inklusive följande krav. Om du inte efterlever alla policykraven kan ditt SDK eller din medlingsplattform tas bort eller stängas av från programmet för självcertifierade annons-SDK:er för familjer.

Du ansvarar för att se till att ditt SDK eller din medlingsplattform uppfyller kraven, så ta dig tid att läsa Google Plays programpolicy för utvecklare, Google Plays familjepolicyer och programmet för självcertifierade annons-SDK:er för familjer.

1. **Annonsinnehåll:** Annonsinnehåll som är tillgängligt för barn måste vara lämpligt för dem.
   - Du måste (i) definiera vad som utgör olämpligt innehåll och beteende och (ii) förbjuda det i dina villkor eller policyer. Definitionerna ska följa Google Plays programpolicy för utvecklare.
   - Du måste även 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 intresseformuläret.
   - Du måste se till att allt annonsmaterial som används i annonsering för barn som säljs via budgivning i realtid har granskats och efterlever kraven ovan.
   - Du måste dessutom ha en mekanism för att visuellt identifiera annonsmaterial från ditt annonsutrymme (till exempel genom att vattenstämpla annonsmaterialet med ditt företags logotyp eller liknande funktioner).
2. **Annonsformat:** Du måste se till att alla annonser som visas för minderåriga användare följer kraven på annonsformat för familjer och att du tillåter att utvecklare väljer annonsformat som efterlever Google Plays familjepolicy.
   - Du får inte visa annonser med hjälp av vilseledande innehåll och de får inte vara utformade på ett sätt som leder till oönskade klick av minderåriga användare. Vilseledande annonser som tvingar användaren att klicka på dem genom att använda en stängningsknapp som utlöser en till annons, eller genom att annonserna plötsligt visas i delar av appen där användaren oftast trycker på en annan funktion, är inte tillåtna.
   - Störande annonser, inklusive sådana som tar upp hela skärmen eller stör normal användning och som inte har något tydligt sätt att stänga annonsen (t.ex. annonsväggar), är inte tillåtna.
   - Annonser som stör normal användning av appar eller spel, inklusive premierade annonser eller annonser med medgivande, som inte går att stänga efter fem sekunder.
   - Flera annonsplaceringar på samma sida är inte tillåtet. Till exempel tillåts inte bannerannonser som visar flera erbjudanden på en placering eller som visar fler än en banner- eller videoannons.
   - Det måste gå att skilja annonserna från annat innehåll i appen på ett tydligt sätt. Offerwalls och helskärmsannonsupplevelser som inte tydligt går att identifiera som annonser av minderåriga användare är inte tillåtna.
   - Användare får inte manipuleras till att titta på annonserna med hjälp av känslomässig utpressning eller stötande innehåll.

3. **IBA/remarketing:** Du måste se till att annonser som visas för minderåriga användare inte omfattar 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).
4. **Datahantering:** Du som SDK-leverantör 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 SDK:et och begränsa användningen av uppgifterna till de syften du har angett. Dessa krav för Google Play gäller utöver de eventuella krav som föreskrivs i tillämpliga integritets- och dataskyddslagar. Du måste meddela om några personliga och känsliga uppgifter samlas in från barn, inbegripet men inte begränsat till autentiseringsuppgifter, sensordata från mikrofoner och kameror, enhetsdata, Android-id och annonsanvändning.
   - Du måste tillåta 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 regler, 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.
   - Du måste se till att budgivarna för allt annonsmaterial som används i annonsering för barn som säljs via budgivning i realtid är medvetna om de särskilda integritetskraven.
   - Du får inte överföra AAID, SIM-serienummer, versionens serienummer, BSSID, MAC-adress, SSID, IMEI-kod och/eller IMSI-nummer från barn eller användare i okänd ålder.
5. **Medlingsplattformar**: Du måste göra följande när du visar annonser för barn:
   - Använd endast självcertifierade annons-SDK:er för familjer 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.
6. **Självcertifiering och efterlevnad:** Du måste ge Google tillräckligt underlag, till exempel genom att skicka in de uppgifter som anges i intresseformuläret , för att verifiera att annons-SDK:et efterlever alla självcertifieringskrav, inbegripet men inte begränsat till följande:
   - Tillhandahåll en version av SDK:ets eller medlingsplattformens användarvillkor, integritetspolicy och utvecklarens integreringsguide på engelska
   - Skicka in en testapp som använder den senaste versionen av annons-SDK:et som uppfyller kraven. Testappen måste vara en komplett och körbar APK-fil som utnyttjar alla funktioner i SDK:et. Krav på testappar:
     - Den måste skickas in som en komplett och körbar APK-fil avsedd att köras på en telefonformfaktor.
     - Det måste vara den senaste versionen av annons-SDK:et eller en version som håller på att släppas måste användas. Annons-SDK:et måste följa Google Plays policyer.
     - Testappen måste använda alla funktioner i annons-SDK:et, inklusive att anropa annons-SDK:et för att hämta och visa annonser.
     - Den måste ha full åtkomst till alla annonsutrymmen som är aktiva eller visas i nätverket via annonsmaterial som begärs via testappen.
     - Den får inte begränsas utifrån geografisk plats.
     - Om ditt annonsutrymme har en blandad målgrupp måste din testapp kunna skilja mellan förfrågningar om annonsmaterial från hela annonsutrymmet och det annonsutrymme som passar barn eller alla åldersgrupper.
     - Den får inte begränsas till specifika annonser i annonsutrymmet om den inte styrs av skärmen för ålderskontroll.

7. Du måste svara inom rimlig tid på eventuella efterföljande förfrågningar om information och självcertifiera att alla nya versioner följer Google Plays senaste programpolicy för utvecklare, inklusive kraven i familjepolicyn.
8. **Juridisk efterlevnad:** Självcertifierade annons-SDK:er för familjer måste ha stöd för visning av annonser som efterlever alla relevanta bestämmelser och förordningar gällande barn som kan tillämpas på deras utgivare.
   - Du måste säkerställa att SDK:et eller medlingsplattformen efterlever den amerikanska lagen COPPA (Children's Online Privacy and Protection Act) , EU:s allmänna dataskyddsförordning (GDPR) och alla andra tillämpliga lagar och förordningar.

     Obs! 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.

Läs sidan för programmet för självcertifierade annons-SDK:er för familjer om du vill veta mer om programkraven.

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 utvecklarwebbplatsen.

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.

Vi tillåter inte appar eller innehåll i appar som undergräver användarnas förtroende för Google Plays ekosystem. När vi bedömer om vi ska erbjuda eller ta bort appar från Google Play tar vi hänsyn till ett antal faktorer som inbegriper 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 inbegriper men inte begränsas till klagomål på en app eller utvecklare, information i nyhetsrapporter, 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

När vi granskar innehåll eller konton för att kontrollera laglighet och efterlevande av våra policyer fattar vi vårt beslut utifrån varierad information, inklusive appens metadata (till exempel appens titel och beskrivning), upplevelsen i appen, kontouppgifter (till exempel tidigare policyöverträdanden), eventuell tredjepartskod i appen och annat som tillhandahållits via rapporteringsmekanismer (om tillämpligt) och granskningar på eget initiativ. Tänk på att du ansvarar för att eventuell tredjepartskod (t.ex. ett SDK) som används i appen, och den tredje partens metoder gällande appen, följer Google Plays programpolicy för utvecklare.

Om appen eller utvecklarkontot 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 ditt konto och i alla dina appar.

Upprepade eller allvarliga överträdelser (till exempel skadlig kod, 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 dina appar på olika sätt. Vi använder både automatiska och manuella utvärderingar för att granska appar och deras innehåll för att identifiera och utvärdera innehåll som strider mot våra policyer och är skadligt för användare och Google Plays ekosystem i stort. Automatiserade modeller hjälper oss att upptäcka fler överträdelser och att bedöma potentiella

problem fortare, så att Google Play kan fortsätta att vara en säker plats för alla. Innehållet som strider mot våra policyer tas antingen bort av våra automatiserade modeller eller, om ett mer nyanserat beslut krävs, så flaggas det för att granskas ytterligare av utbildade operatörer och analytiker som utvärderar innehållet, till exempel då en förståelse av innehållets sammanhang är nödvändig. Resultatet av dessa manuella granskningar används för att bygga upp träningsdata och förbättra våra maskininlärningsmodeller.

I följande avsnitt beskrivs vilka åtgärder Google Play kan vidta och hur dessa påverkar din app och/eller ditt utvecklarkonto på Google Play.

Om inget annat meddelas om tillämpning så påverkar dessa åtgärder alla regioner. Om appen exempelvis blir avstängd så är den inte tillgänglig i några regioner. Dessutom gäller dessa åtgärder om inget annat anges, såvida du inte överklagar dem och ditt överklagande godkänns.

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 har tagits bort kan användarna inte se appens butiksuppgifter. 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.
- 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.
- 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.

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.
- 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.

Regionsbegränsning

- Din app kan bara laddas ned via Google Play av användare i vissa regioner.
- Appen går inte att hitta i Play Butik för användare från andra regioner.
- Användare som har installerat appen tidigare kan fortsätta att använda den på sin enhet men får inte längre några uppdateringar.
- Att du begränsar appen till vissa regioner påverkar inte statusen för ditt utvecklarkonto på Google Play.

När kontot har begränsats

- När ditt utvecklarkonto har begränsats tas alla appar i din katalog bort från Google Play och du kan inte längre publicera nya appar eller publicera befintliga appar på nytt. Du har fortfarande åtkomst till Play Console.
- Eftersom alla appar tas bort kommer användare inte att kunna se appens butiksuppgifter och din utvecklarprofil.
- Dina nuvarande användare kommer inte att kunna göra några köp i appen eller använda några faktureringsfunktioner i dina appar.
- Du kan fortfarande använda Play Console för att skicka mer information till Google Play och ändra informationen för kontot.
- Du kan publicera dina appar på nytt när du har åtgärdat alla överträdelser av policyn.

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 och din utvecklarprofil.
- Dina nuvarande användare kommer inte att kunna göra några köp i appen eller använda några faktureringsfunktioner i dina appar.

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.

Inaktiva konton

Inaktiva konton är utvecklarkonton som inte har använts på länge eller är övergivna. Inaktiva konton har inte den goda status som krävs i distributionsavtalet för utvecklare .

Utvecklarkonton på Google Play är avsedda för aktiva utvecklare som publicerar och kontinuerligt underhåller sina appar. Vi stänger konton som är inaktiva eller inte används regelbundet på ett betydelsefullt sätt (till exempel för att publicera och uppdatera appar, komma åt statistik eller hantera butiksuppgifter) för att förhindra missbruk.

Om ditt inaktiva konto stängs raderas kontot och all data som är kopplad till det. Registreringsavgiften betalas inte tillbaka. Innan vi stänger ditt inaktiva konto meddelar vi dig med hjälp av kontaktuppgifterna i kontot.

Om du tidigare har haft ett inaktivt konto som stängts kan du skapa ett nytt konto om du bestämmer dig för att publicera på Google Play. Det går inte att återaktivera kontot och du får inte tillgång till

appar och data från det i det nya kontot.

Hantera och rapportera policyöverträdelser

Överklaga en tillämpningsåtgärd

Vi återställer appar om det har skett ett misstag och en ny granskning visar att appen inte bryter mot programpolicyn för Google Play eller 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 eller klickar här 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 . Vi kan dock inte erbjuda juridisk rådgivning. Om du behöver juridisk rådgivning rekommenderar vi att du kontaktar en jurist.

- Appverifiering
- 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

---

Krav för Play Console

För att upprätthålla säkerheten i vårt mångsidiga ekosystem för appar kräver Google Play att alla utvecklare slutför Play Consoles krav, inklusive för alla profiler som är länkade till ditt utvecklarkonto på Play Console. Verifierade uppgifter visas på Google Play för att underlätta användarnas tillit för utvecklarna. Läs mer om informationen som visas på Google Play.

Du kan välja mellan två typer av utvecklarkonton på Google Play: personligt konto och organisationskonto. Att välja rätt utvecklarkonto och slutföra nödvändiga verifieringar är avgörande för en smidig onboarding. Läs mer om hur du väljer en typ av utvecklarkonto.

Utvecklare som skapar ett Play Console-konto och tillhandahåller följande tjänster måste registreras som en organisation:

- Finansiella produkter och tjänster, inbegripet men inte begränsat till banker, lån, aktiehandel, investeringsfonder, mjukvaruplånböcker för kryptovaluta och kryptobörser. Läs mer om policyn för finansiella tjänster.
- Hälsoappar, till exempel medicinska appar och appar för forskning med försökspersoner. Läs mer om hälsoappskategorier.
- Appar godkända för klassen VpnService . Läs mer om VPN-tjänstpolicyn.
- Myndighetsappar, inklusive appar som utvecklas av eller för en myndighet.

När du har valt kontotyp måste du

- tillhandahålla korrekta uppgifter om utvecklarkontot, inklusive följande:
  - officiellt namn och officiell adress
  - DUNS-nummer , om registreringen är för en organisation
  - e-postadress och telefonnummer för kontakt
  - utvecklarens e-postadress och telefonnummer som visas på Google Play, om tillämpligt
  - betalningsmetoder, om tillämpligt

- Google-betalningsprofil som är länkad till ditt utvecklarkonto.
- Om registreringen är för en organisation ska du se till att uppgifterna för utvecklarkontot är aktuella och stämmer överens med uppgifterna i Dun & Bradstreet-profilen.

Innan du skickar in appen ska du

- tillhandahålla all appinformation och metadata på ett korrekt sätt
- ladda upp appens integritetspolicy och fylla i uppgifterna som krävs i avsnittet om datasäkerhet
- tillhandahålla ett aktivt demokonto, inloggningsinformation och alla andra resurser som krävs för att Google Play ska kunna granska appen (dvs. inloggningsuppgifter, QR-kod osv.).

Du ska som vanligt se till att användarupplevelsen i appen är stabil, engagerande och följsam. Kontrollera att allt i appen, inklusive annonsnätverk, analystjänster och SDK:er från tredje part efterlever Google Plays programpolicy för utvecklare och om barn ingår i appens målgrupp ska du se till att efterleva familjepolicyn.

Kom ihåg att du ansvarar för att granska distributionsavtalet för utvecklare och alla programpolicyer för utvecklare för att se till att appen efterlever dessa.

Developer Distribution Agreement

Behöver du mer hjälp?

Testa detta härnäst:

Kontakta oss

Berätta mer så hjälper vi dig