

Programpolitik for udviklere (gyldig fra 1. oktober 2020)

Lad os skabe verdens mest sikre kilde til apps og spil

Det er din innovation, der skaber vores fælles succes. Men der medfølger et ansvar. Disse Programpolitikker for udviklere og [Distributionsaftale for udviklere](#) sikrer, at vi sammen kan fortsætte med at levere verdens mest innovative og sikre apps til over en milliard brugere via Google Play. Nedenfor kan du se nærmere på vores politikker.

Begrænset indhold

Folk fra hele verden bruger Google Play til at få adgang til apps og spil hver eneste dag. Før du indsender en app, skal du vurdere, om din app er relevant for Google Play, og om den overholder den lokale lovgivning.

Fare for børn

Apps med indhold, der seksualiserer mindreårige, fjernes omgående fra Play Butik-, herunder, men ikke begrænset til, apps, der promoverer pædofili eller upassende interaktioner, der er målrettet mod mindreårige (f.eks. befamling eller kæleri).

Derudover er apps, der er henvendt til børn, men indeholder voksentemaer, ikke tilladt, herunder, men ikke begrænset til, apps med overdreven vold, blod og blodsudgydelse og apps, der afbilder eller opfordrer til skadelige og farlige aktiviteter. Vi tillader heller ikke apps, der promoverer et negativt krops- eller selv billede, herunder apps, der med underholdningsformål viser plastikkirurgi, væggtab og andre kosmetiske indgreb målrettet en persons fysiske udseende.

Hvis vi får kendskab til indhold med billeder, der viser seksuelt misbrug af børn, anmelder vi det til de relevante myndigheder og sletter de Google-konti, der tilhører de personer, der har været involveret i distributionen af billederne.

Upassende indhold

Vi vil sikre, at Google Play forbliver en sikker og respektfuld platform, og derfor har vi oprettet standarder, som definerer og forbyder indhold, som er skadeligt eller upassende for vores brugere.

Seksuelt indhold og ukvemsord

Vi tillader ikke apps, der indeholder eller promoverer seksuelt indhold eller ukvemsord, herunder pornografi eller indhold eller tjenester, der er beregnet til at være seksuelt tilfredsstillende. Indhold, der omfatter nøgenhed, kan tillades, hvis det primære formål er uddannelsesmæssigt, dokumentarisk, videnskabeligt eller kunstnerisk, og det ikke er umotiveret.

Her er nogle eksempler på typiske overtrædelser:

- Afbildninger af seksuel nøgenhed eller seksuelt ladede positurer, hvor personen er nøgen, sløret eller minimalt påklædt, og/eller hvor beklædningen ikke ville være acceptabel i en passende offentlig sammenhæng.
- Afbildninger, animationer eller illustrationer af sexscener, seksuelt ladede positurer eller seksuel afbildning af kropsdele.
- Indhold, som afbilder eller er funktionelle seksuelle hjælpemidler, sexvejledninger, ulovlige seksuelle temaer og feticher.
- Indhold, der er uanstændigt eller underlødigt – herunder, men ikke begrænset til, indhold, der indeholder ukvemsord, nedsættende bemærkninger, udpenslet tekst om upassende emner eller voksenrettede/seksuelle søgeord på profilsiden i Play Butik eller i appen.
- Indhold, som afbilder, beskriver eller opfordrer til seksuel omgang med dyr.
- Apps, der promoverer sexrelateret underholdning, escortservice eller andre tjenester, der kan fortolkes som ydelse af seksuelle handlinger mod kompensation.
- Apps, der nedgør eller objektiviserer personer.

Hadefulde ytringer

Vi tillader ikke apps, der ansporer til vold eller had mod enkeltpersoner eller grupper af personer på baggrund af deres race eller etniske tilhørsforhold, religion, handicap, alder, nationalitet, veteranstatus, seksuelle orientering, køn, kønsidentitet eller nogen andre kendetegn, der er forbundet med systematisk diskrimination eller marginalisering.

Apps, der indeholder undervisningsrettet, dokumentarisk, videnskabeligt eller kunstnerisk indhold, der er relateret til nazister, blokeres muligvis i visse lande i overensstemmelse med lokale love og bestemmelser.

Her er eksempler på typiske overtrædelser:

- Indhold eller tale, der hævder, at en beskyttet gruppe er umenneskelig, underlegen eller bør udsættes for had.
- Apps, der indeholder hadefulde, nedsættende udtryk eller teorier om, at en beskyttet gruppe besidder negative egenskaber (f.eks. at gruppen er ondsindet, korrupt, skadelig), eller som direkte eller indirekte hævder, at gruppen er en trussel.
- Indhold eller ytringer, der forsøger at opfordre andre til at tro, at nogle mennesker skal udsættes for had eller diskrimination, fordi de er medlem af en beskyttet gruppe.
- Indhold, der promoverer hadesymboler, f.eks. flag, symboler, insignier, remedier eller adfærd, der er knyttet til hadegrupper.

Vold

Vi tillader ikke apps, der afbilder eller formidler umotiveret vold eller andre farlige aktiviteter. Apps, der skildrer fiktiv vold i forbindelse med et spil, f.eks. tegnefilm, jagt eller fiskeri, er generelt tilladt.

Her er nogle eksempler på typiske overtrædelser:

- Detaljerede afbildninger eller beskrivelser af realistisk vold eller voldelige trusler mod en person eller et dyr.
- Apps, der opfordrer til selvskade, selvmord, mobning, chikane, spiseforstyrrelser, kvælningslege eller andre handlinger, der kan resultere i alvorlige fysiske skader eller død.

Terrorrelateret indhold

Vi tillader ikke terrororganisationer at udgive apps i Google Play til noget formål, herunder rekruttering.

Vi tillader ikke apps med terrorrelateret indhold, f.eks. indhold, som fremmer terrorhandling, ansporer til vold eller hylder terrorangreb. Vær opmærksom på at give nok oplysninger og dermed hjælpe brugerne til at forstå sammenhængen, hvis indsendelse af terrorrelateret indhold sker i en uddannelsesmæssig, dokumentarisk, videnskabelig eller kunstnerisk sammenhæng.

Følsomme begivenheder

Vi tillader ikke apps, der udnytter eller udviser mangel på sympati i forbindelse med en naturkatastrofe, grusomheder, konflikt, død eller andre tragiske hændelser. Apps med indhold, der er relateret til en følsom begivenhed, er generelt tilladt, hvis indholdet er undervisningsrettet, dokumentarisk, videnskabeligt eller kunstnerisk eller har til hensigt at advare brugerne om eller øge bevidstheden om den følsomme begivenhed.

Her er eksempler på typiske overtrædelser:

- Manglende respekt i forbindelse med en virkelig persons eller gruppes død på grund af selvmord, overdosis, naturlige årsager osv.
- Benægtelse af en større tragisk hændelse.
- Tilsyneladende at profitere på en tragisk hændelse, uden at det gavner ofrene mærkbart.

Mobning og chikane

Vi tillader ikke apps, der indeholder eller formidler trusler, chikane eller mobning.

Her er eksempler på typiske overtrædelser:

- Mobning af ofre for internationale eller religiøse konflikter.
- Indhold, der har til formål at udnytte andre, f.eks. afpresning o.l.
- Opslag af indhold for at ydmyge nogen offentligt.
- Chikanering af ofre for en tragisk hændelse eller af ofrenes venner og familie.

Farlige produkter

Vi tillader ikke apps, som muliggør salg af sprængstoffer, skydevåben, ammunition og noget tilhører til skydevåben.

- Begrænset tilhører omfatter tilhører, der gør det muligt at få skydevåben til at simulere automatisk skud, eller som omdanner et skydevåben, så det får automatisk skydefunktion (f.eks. bump stocks, gatling-aftrekkere, automatiske arme til indlægning og konverteringssæt) samt magasiner eller bælt med mere end 30 patroner.

Vi tillader ikke apps med instruktioner i fremstilling af sprængstof, skydevåben, ammunition, begrænset skydevåbentilhører eller andre våben. Dette omfatter også instruktioner i, hvordan man ændrer på et skydevåben, så det får automatisk eller simuleret automatisk skydefunktion.

Marihuana

Vi tillader ikke apps, som muliggør salg af marihuana eller marihuanaprodukter uanset lovlighed.

Her er nogle eksempler på typiske overtrædelser:

- Give brugere mulighed for at bestille marihuana via en indkøbsfunktion i appen.
- Hjælpe brugere med at arrangere levering eller afhentning af marihuana.
- Muliggøre salg af produkter, der indeholder THC (tetrahydrocannabinol), herunder produkter som f.eks. CBD-olier, der indeholder THC.

Tobak og alkohol

Vi tillader ikke apps, som muliggør salg af tobak (herunder e-cigaretter) eller opfordrer til ulovlig eller upassende brug af alkohol eller tobak.

Her er eksempler på typiske overtrædelser:

- Afbildninger eller opfordring til brug eller salg af alkohol eller tobak rettet mod mindreårige.
- Antyde, at forbrug af tobak kan forbedre sociale, seksuelle, professionelle, intellektuelle eller atletiske egenskaber.
- Positiv skildring af overdreven druk, herunder positiv skildring af overdreven druk, fuldskab og drikkekonkurrencer.

Finansielle tjenester

Vi tillader ikke apps, der udsætter brugerne for vildledende eller skadelige finansielle produkter og ydelser.

I forbindelse med denne politik er finansielle produkter og ydelser defineret som nogen, der er relateret til administration eller investering af penge og kryptovalutaer. Dette omfatter også personlig rådgivning.

Hvis din app indeholder eller promoverer finansielle produkter og ydelser, skal du overholde den nationale og lokale lovgivning i det område eller land, som din app henvender sig til. Dette kan f.eks. være at inkludere specifikke oplysninger, der er påkrævet af lokal lovgivning.

Binære optioner

Vi tillader ikke apps, der giver brugerne mulighed for at handle med binære optioner.

Kryptovalutaer

Vi tillader ikke apps, som udvinder kryptovaluta på enheder. Apps, der fjernadministrerer udvinding af kryptovaluta, er tilladt.

Privatlån

Privatlån defineres som udlån af penge fra en enkeltperson, en organisation eller en part til en individuel forbruger på engangsbasis og ikke med henblik på finansiering af anlægsaktiver eller uddannelse. Forbrugere, der optager privatlån, har brug for oplysninger om lånemulighedernes kvalitet, elementer, gebyrer, afdragsplan, risici og fordele for at kunne træffe en velovervejede beslutning om, hvorvidt de skal optage lånet.

- Eksempler: Privatlån, kviklån, P2P-lån eller lån med pant i bil
- Dette omfatter ikke: Boliglån, billån, studielån eller kassekredit (såsom kreditkort og kreditgrænser)

Apps, der tilbyder privatlån, herunder, men ikke begrænset til, apps, der tilbyder direkte lån og genererer kundeemner, samt apps, der skaber forbindelse mellem forbrugere og tredjepartslångivere, skal oplyse følgende i appens metadata:

- Minimum- og maksimumperiode for tilbagebetaling
- Årlige omkostninger i procent (ÅOP), som generelt omfatter rentesatsen plus gebyrer og andre omkostninger på årsbasis, eller en tilsvarende sats, der er beregnet i overensstemmelse med lokal lovgivning
- Et repræsentativt eksempel på lånets samlede omkostninger, inklusive alle relevante gebyrer
- En privatlivspolitik, der detaljeret beskriver, hvordan personlige og følsomme brugerdata bliver tilgået, indsamlet, brugt og delt.

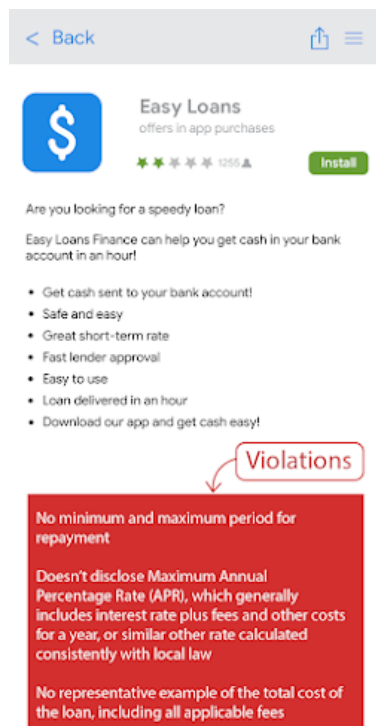
Vi tillader ikke apps, der promoverer privatlån, som kræver fuld tilbagebetaling inden for 60 dage eller derunder fra datoen, hvor lånet udstedes (vi benævner disse "kortfristede privatlån").

Privatlån med høj ÅOP

I USA tillader vi ikke apps til privatlån, hvor de årlige omkostninger i procent (ÅOP) er 36 % eller derover. Apps til privatlån i USA skal angive deres maksimale ÅOP, som er beregnet i overensstemmelse med loven [Truth in Lending Act \(TILA\)](#).

Denne politik gælder for apps, der tilbyder direkte lån og genererer kundeemner samt apps, der forbinder forbrugere med tredjepartslångivere.

Her er eksempler på typiske overtrædelser:



Hasardspil, spil og konkurrencer med rigtige penge

Vi tillader apps med hasardspil med rigtige penge, annoncer med relation til hasardspil med rigtige penge og apps med daglig fantasy-sport, der opfylder visse krav.

Apps med hasardspil

Vi tillader kun indhold og tjenester, der muliggør online hasardspil i:

- Storbritannien, Irland og Frankrig
- Brasilien (begrænset til godkendte apps, der er udgivet af Caixa Economica Federal)

Disse apps skal opfylde følgende krav:

- Udvikleren skal [gennemføre ansøgningsprocessen](#) for at kunne distribuere appen i Play
- Appen skal overholde alle gældende love og branchestandarder for hvert af de lande, hvor den distribueres
- Udvikleren skal have en gyldig licens til hasardspil for hvert af de lande, hvor appen distribueres
- Appen skal forhindre mindreårige brugere i at spille hasardspil i appen
- Appen skal forhindre brug fra lande, der ikke er dækket af licensen til hasardspil, som udvikleren har indsendt
- Appen må IKKE kunne købes som købeapp i Google Play, og den må heller ikke benytte Google Play Fakturering i appen
- Appen skal kunne downloades og installeres gratis via Play Butik
- Appen skal være klassificeret som "AO" (Adult Only, kun for voksne) eller en tilsvarende IARC-klassificering
- Appen og den tilhørende appfortegnelse skal tydeligt vise oplysninger om ansvarligt hasardspil.

Alle andre steder tillader vi ikke indhold og tjenester, der formidler hasardspil på nettet, herunder, men ikke begrænset til, onlinekasinoer, sportsvæddemål og lotterier samt færdighedsspil med kontantpræmier eller andre præmier af værdi i den virkelige verden.

Andre spil, konkurrencer eller turneringer med rigtige penge

Vi tillader ikke indhold eller tjenester, der giver brugerne mulighed for at satse, investere eller deltage med rigtige penge (herunder produkter i apps, der købes med penge) for at få en præmie med reel pengeværdi. Dette omfatter, men er ikke begrænset til, onlinekasinoer, sportsvæddemål, lotterier, der ikke opfylder kravene til de ovennævnte hasardspilapps og spil, der tilbyder præmier med kontanter eller anden reel værdi.

Her er eksempler på overtrædelser:

- Spil, der accepterer penge i bytte for muligheden for at vinde en fysisk præmie eller pengepræmie
- Spil med "loyalitetspoint" (f.eks. engagement eller aktivitet), der (1) genereres eller øges via køb med rigtige penge, som (2) kan byttes med varer eller præmier af reel pengeværdi
- Apps, der accepterer eller administrerer hasardspil med væddemål, valuta i appen, der er påkrævet for at deltage, gevinster eller krav om depositummer for at få adgang til eller blive bedre kvalificeret til en fysisk præmie eller pengepræmie
- Apps, der opfordrer brugeren til at handle ved at satse, investere eller deltage i spil, konkurrencer eller turneringer med rigtige penge, f.eks. apps med navigationselementer (menupunkter, faner, knapper osv.), der inviterer brugeren til at deltage i en turnering med mulighed for at vinde en pengepræmie ved hjælp af opfordringer som f.eks. "TILMELD DIG" eller "DELTA I KONKURRENCEN".

Annoncer for hasardspil eller andre spil, konkurrencer eller turneringer med rigtige penge i apps, der distribueres via Play

Vi tillader apps, der annoncerer for hasardspil eller andre spil, konkurrencer eller turneringer med rigtige penge, hvis de lever op til følgende krav:

- Appen og annoncen (samt annoncøren) skal overholde alle gældende love og branchestandarder for alle steder, hvor annoncen vises
- Annoncen skal opfylde de lokale licenskrav for alle promoverede hasardspilrelaterede produkter og tjenester
- Appen må ikke vise en hasardspilannonce til personer, der vides at være under 18 år
- Appen må ikke være tilmeldt programmet For hele familien
- Appen må ikke være målrettet mod personer under 18 år
- Hvis der annonceres for en hasardspilapp (som defineret ovenfor), skal annoncen tydeligt vise oplysninger om ansvarligt hasardspil på landingssiden, i den annoncerede appfortegnelse eller i appen-
- Appen må ikke levere simuleret hasardspilindhold (f.eks. apps til sociale kasinoer og apps med virtuelle spillemaskiner)
- Appen må ikke levere funktioner, som understøtter hasardspil eller andre spil, lotterier eller turneringer med rigtige penge (f.eks. funktioner, der hjælper med væddemål, udbetalinger, overvågning af sportsresultater/odds eller administration af deltagelsesfinansiering)
- Du må ikke have en ejerandel i hasardspiltjenester eller andre tjenester til spil, lotterier eller turneringer med rigtige penge, der annonceres for i appen
- Appindhold må ikke promovere eller dirigere brugere til hasardspil eller andre spil, lotterier eller turneringer med rigtige penge

Det er kun hasardspilapps (som defineret ovenfor) eller apps, der opfylder alle disse krav til hasardspilannoncer, der må indeholde annoncer for hasardspil med rigtige penge eller spil, lotterier eller turneringer med rigtige penge.

Her er nogle eksempler på overtrædelser:

- En app, der er udviklet til mindreårige brugere og viser en annonce, som promoverer hasardspiltjenester
- Et simuleret kasinospil, der promoverer eller dirigerer brugerne til kasinoer med rigtige penge
- En app dedikeret til overvågning af sportsodds, der indeholder integrerede spilannoncer med links til websites for sportsvæddemål
- En nyhedsapp, der viser annoncer for en hasardspiltjeneste, som ejes eller drives af appens udvikler
- Apps med hasardspilannoncer, der overtræder vores politik om [vildledende annoncer](#), f.eks. annoncer, der vises for brugerne som knapper, ikoner eller andre interaktive elementer i apps

Apps med daglig fantasy-sport

Vi tillader kun apps med daglig fantasy-sport, som defineret i gældende lokal lovgivning, hvis de lever op til følgende krav:

- 1) Appen distribueres enten kun i USA, eller 2) appen er kvalificeret i henhold til de ovennævnte krav til hasardspilapps
- Udvikleren skal gennemføre [ansøgningsprocessen for daglig fantasy-sport](#) og godkendes for at kunne distribuere appen i Play
- Appen skal overholde alle gældende love og branchestandarder for de lande, hvor den distribueres
- Appen skal forhindre mindreårige brugere i at indgå væddemål eller foretage pengetransaktioner i appen

- Appen må IKKE kunne købes som købeapp i Google Play, og den må heller ikke benytte Google Play Fakturering i appen
- Appen skal kunne downloades og installeres gratis i Play Butik
- Appen skal være klassificeret "AO" (Adult Only, kun for voksne) eller en tilsvarende IARC-klassificering
- Appen og den tilhørende appfortegnelse skal tydeligt vise oplysninger om ansvarligt hasardspil

Hvis appen distribueres i USA, gælder følgende yderligere krav:

- Appen skal overholde alle gældende love og branchestandarder for den delstat eller det område i USA, hvor den distribueres
- Udvikleren skal have en gyldig licens for hver stat eller hvert område i USA, hvor der kræves en licens til apps med daglig fantasy-sport
- Appen skal forhindre brug i amerikanske stater og områder, hvor udvikleren ikke har den krævede licens til apps med daglig fantasy-sport
- Appen skal forhindre brug i amerikanske stater og områder, hvor apps med daglig fantasy-sport ikke er lovlige

Ulovlige aktiviteter

Vi tillader ikke apps, der formidler eller promoverer ulovlige aktiviteter.

Her er nogle eksempler på typiske overtrædelser:

- Formidling af salg eller køb af ulovlige stoffer eller salg af receptpligtig medicin uden en recept.
- Afbildninger eller opfordring til brug af stoffer, alkohol eller tobak rettet mod mindreårige.
- Vejledning i dyrkning eller fremstilling af ulovlige stoffer.

Brugergenereret indhold

Brugergenereret indhold er indhold, som brugere leverer til en app, og som er synligt eller tilgængeligt for i hvert fald en del af appens brugere.

Apps med brugergenereret indhold skal:

- Kræve, at brugerne accepterer appens servicevilkår og/eller brugerpolitik, før de kan oprette eller uploade brugergenereret indhold
- Definere stødende indhold og adfærd (på en måde, der overholder Plays programpolitikker for udviklere) og forbyde dem i appens servicevilkår eller brugerpolitikker
- Implementere stabil, effektiv og løbende moderering af brugergenereret indhold, i et omfang som er rimeligt og svarer til de typer brugergenereret indhold, som hostes i appen
 - I apps med livestreaming skal problematisk brugergenereret indhold fjernes i så tæt på realtid som muligt
 - I apps med augmented reality (AR) skal moderering af brugergenereret indhold (herunder rapporteringssystemet i appen) tage højde for både stødende brugergenereret AR-indhold (f.eks. et eksplicit seksuelt AR-billede) og følsom placering af AR-forankring (f.eks. AR-indhold, der er forankret til et begrænset område, f.eks. en militærbase eller en privat ejendom, hvor AR-forankring kan forårsage problemer for ejeren af ejendommen)
- Sørge for et brugervenligt system i appen til rapportering af problematisk brugergenereret indhold og skride til handling mod brugergenereret indhold, hvor dette er passende
- Fjerne eller blokere brugere, der overtræder servicevilkårene og/eller brugerpolitikken for appen
- Træffe sikkerhedsforanstaltninger for at forhindre indtægtsgenerering i appen via tilskyndelser til uhensigtsmæssig brugeradfærd

Apps, hvis primære formål er at vise problematisk brugergenereret indhold, fjernes fra Google Play. Også apps, der er endt med primært at blive brugt til at hoste problematisk brugergenereret indhold, eller som udvikler et ry blandt brugere som et sted, der er godt for denne type indhold, fjernes fra Google Play.

Her er nogle eksempler på typiske overtrædelser:

- Promovering af brugergenereret eksplicit indhold af seksuel karakter, herunder implementering af eller tilladelse til betalte funktioner, der hovedsageligt tilskynder til deling af uhensigtsmæssigt indhold.
- Apps med brugergenereret indhold, der mangler tilstrækkelige sikkerhedsforanstaltninger mod trusler, chikane eller mobning, i særdeleshed mod mindreårige.
- Indlæg, kommentarer eller billeder i en app, som primært er beregnet til at chikanere eller udstille en anden person til misbrug, grove angreb eller latterliggørelse.
- Apps, hvor der gentagne gange ikke reageres på klager fra brugerne over problematisk indhold.

Ikke-godkendte lægemidler

Google Play tillader ikke apps, som promoverer eller sælger ikke-godkendte lægemidler, uanset påstande om lovlighed.

Eksempler:

- Alle varer på denne ikke-udtømmende liste over [forbudte lægemidler og kosttilskud](#)
- Produkter, der indeholder Ephedra
- Produkter, der indeholder humant choriongonadotropin (hCG) i forbindelse med vægttab eller vægtkontrol, eller når de promoveres sammen med anabolske steroider
- Urte- og diættilskud med aktive farmaceutiske eller farlige stoffer
- Falske eller vildledende sundhedsanprisninger, herunder påstande om, at et produkt er lige så effektivt som receptpligtig medicin eller kontrollerede stoffer
- Produkter, der ikke er godkendt af myndighederne, og som markedsføres på en måde, der antyder, at de er sikre eller effektive at anvende til forebyggelse, helbredelse eller behandling af en bestemt sygdom eller lidelse
- Produkter, der har været genstand for myndigheds- eller lovindgreb eller advarsler
- Produkter med navne, der til forveksling ligner et ikke-godkendt lægemiddel, kosttilskud eller kontrolleret stof

Du kan få yderligere oplysninger om de ikke-godkendte eller vildledende lægemidler og kosttilskud, som vi overvåger, på www.legitscript.com.

Intellectuel ejendom

Når udviklere kopierer en andens værk eller bruger det uden den nødvendige tilladelse, kan det skade ejeren af det pågældende værk. Brug ikke andres værker på uretfærdig vis.

Intellectuel ejendom

Vi tillader ikke apps eller udviklerkonti, som krænker andres intellektuelle ejendomsrettigheder (herunder varemærker, ophavsret, patenter, forretningshemmeligheder og andre ejendomsrettigheder). Vi tillader heller ikke apps, der opfordrer til eller forårsager krænkelser af intellektuelle ejendomsrettigheder.

Vi reagerer på klare meddelelser om påstået krænkelser af ophavsretten. Hvis du vil have flere oplysninger eller indsende en DMCA-anmodning, kan du læse vores [procedurer vedrørende ophavsret](#).

Hvis du vil indsende en klage vedrørende salg eller promovering af kopivarer i en app, skal du indsende en [meddelelse om forfalskning](#).

Hvis du er varemærkeindehaver og mener, at der er en app i Google Play, som krænker dine varemærkerettigheder, anbefaler vi, at du kontakter udvikleren direkte for at løse problemet. Hvis du ikke kan nå til enighed med udvikleren, kan du indsende en varemærkeklage ved hjælp af denne [formular](#).

Hvis du har skriftlig dokumentation på, at du har tilladelse til at anvende en tredjeparts intellektuelle ejendom i din app eller profilside i Play Butik (f.eks. brandnavne, logoer og grafiske aktiver), skal du [kontakte Google Play-teamet](#) forud for din indsendelse for at sikre, at din app ikke afvises som følge af krænkelser af intellektuelle ejendomsrettigheder.

Uautoriseret brug af ophavsretsligt beskyttet indhold

Vi tillader ikke apps, der krænker ophavsretten. Modificering af ophavsretsligt indhold kan stadig medføre en overtrædelse. Udviklere kan blive påkrævet at fremlægge bevis på, at de har ret til at bruge ophavsretsligt beskyttet indhold.

Vær forsigtig, når du bruger ophavsretsligt beskyttet indhold til at demonstrere funktioner i din app. Den sikreste fremgangsmåde er generelt at skabe originalt indhold.

Her er nogle eksempler på ophavsretsligt indhold, som ofte anvendes uautoriseret eller på ulovlig vis:

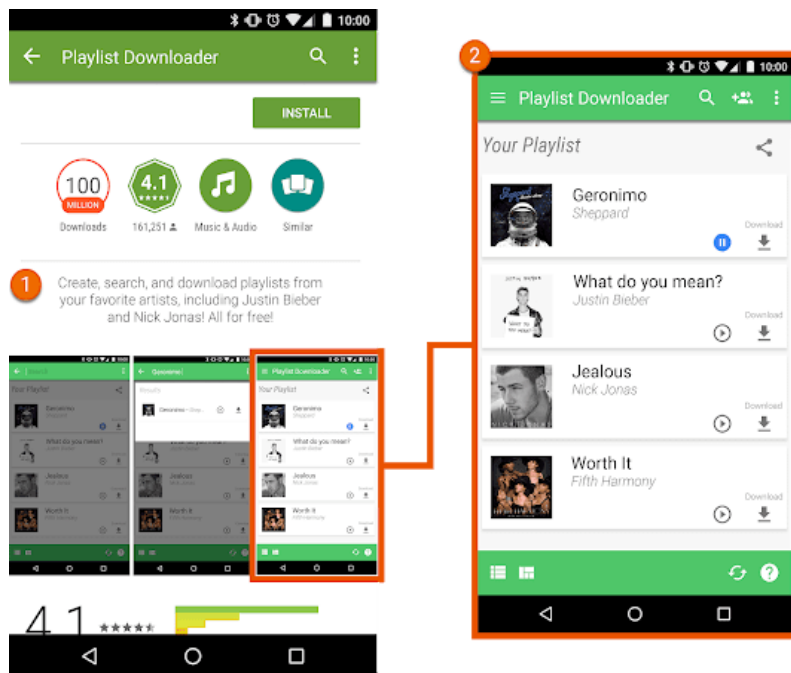
- Forsidebillede til musikalbum, videospil og bøger.
- Billeder fra markedsføringsmateriale til film, tv-serier eller videospil.
- Plakater eller billeder fra tegneserier, tegnefilm, film, musikvideoer eller tv-serier.
- Logoer for professionelle og semiprofessionelle sportshold.
- Billeder, der er taget fra en offentlig persons konto på et socialt medie.
- Professionelle billeder af offentlige personer.
- Reproduktioner eller "fan art", der ikke kan skelnes fra det originale værk, som er beskyttet af ophavsret.
- Apps, der indeholder soundboards til afspilning af lydklip fra ophavsretsligt indhold.
- Komplette reproduktioner eller oversættelser af bøger, som ikke er offentligt tilgængelige.

Opfordring til krænkelse af ophavsretten

Vi tillader ikke apps, som forårsager eller opfordrer til krænkelse af ophavsretten. Før du udgiver din app, skal du undersøge, om appen kan opfordre til krænkelse af ophavsretten og om nødvendigt søge juridisk bistand.

Her er nogle eksempler på typiske overtrædelser:

- Streamingapps, der giver brugerne mulighed for at downloade en lokal kopi af ophavsretsligt beskyttet indhold uden tilladelse.
- Apps, der opfordrer brugerne til at streame og downloade ophavsretsligt beskyttede værker, herunder musik og video, der overtræder gældende lovgivning om ophavsret:



① Beskrivelsen i denne appfortegnelse opfordrer brugerne til at downloade ophavsretsligt beskyttet indhold uden tilladelse.

② Screenshottet i denne appfortegnelse opfordrer brugerne til at downloade ophavsretsligt beskyttet indhold uden tilladelse.

Krænkelse af varemærker

Vi tillader ikke apps, der krænker andres varemærker. Et varemærke er et ord, et symbol eller en kombination af disse, der identificerer kilden til en vare eller tjeneste. Når varemærket er erhvervet, giver det ejeren eksklusive rettigheder til brug af varemærket med hensyn til disse varer eller tjenester.

Der er tale om krænkelse af varemærker ved forkert eller uautoriseret brug af et identisk eller lignende varemærke på en måde, der sandsynligvis vil skabe forvirring om kilden til det pågældende produkt. Hvis din app anvender en anden parts varemærker på en måde, der sandsynligvis vil skabe forvirring, kan din app suspenderes.

Forfalskning

Vi tillader ikke apps, som sælger eller promoverer forfalskede varer. Forfalskede varer er udstyret med et varemærke eller logo, der er identisk med eller i det væsentlige ikke kan skelnes fra en andens varemærke. De efterligner produktets brandelementer i et forsøg på at udgive sig for at være ægte produkter fra brandindehaveren.

Privatliv, vildledning og misbrug af enheder

Det er vigtigt for os at beskytte vores brugeres privatliv og skabe et trygt miljø for dem. Apps, som er vildledende, skadelige eller har til formål at misbruge et netværk, en enhed eller personlige data, er strengt forbudt.

Brugerdata

Det skal være gennemsigtigt, hvordan du håndterer brugerdata (f.eks. oplysninger, der indsamles fra eller omhandler en bruger, herunder enhedsoplysninger). Det betyder, at du skal beskrive, hvordan din app får adgang til, indsamler, bruger og

delers data, samt begrænse brugen af disse data af de beskrevne årsager. Hvis din app desuden håndterer personlige eller følsomme brugerdata, skal du også henvise til de yderligere krav i afsnittet "Personlige og følsomme oplysninger" nedenfor. Disse Google Play-krav er i tillæg til alle krav, der er foreskrevet af gældende love om beskyttelse af personlige oplysninger og data.

Personlige og følsomme oplysninger

Personlige og følsomme brugerdata omfatter, men er ikke begrænset til, personhenførbare oplysninger, økonomiske oplysninger og betalingsoplysninger, godkendelsesoplysninger, telefonbog, data om kontakter, [enhedsplacering](#), oplysninger om sms-beskeder og opkald, mikrofon, kamera samt andre følsomme enheds- og brugsdata. Hvis din app håndterer følsomme brugerdata, skal du gøre følgende:

- Begrænse din adgang, indsamling, brug og deling af personlige eller følsomme oplysninger, der erhverves via appen, til formål, der er direkte forbundet med levering og forbedring af appens funktioner (f.eks. brugerforventet funktionalitet, der dokumenteres og promoveres i appens beskrivelse i Play Butik). Apps, der udvider brugen af disse data til annoncevisning, skal overholde vores [annoncepolitik](#).
- Angive en privatlivspolitik i både det specificerede felt i Play Console og i selve appen. Privatlivspolitikken skal, sammen med eventuelle erklæringer i appen, tydeligt oplyse om, hvordan din app har adgang til, indsamler, anvender og deler brugerdata. Din privatlivspolitik skal oplyse, hvilke typer af personlige og følsomme oplysninger din app har adgang til, indsamler, bruger og deler, samt hvilke typer af parter personlige eller følsomme brugerdata deles med.
- Håndtere alle personlige eller følsomme brugerdata på sikker vis, bl.a. ved at sende dem via moderne kryptering (f.eks. via HTTPS).
- Bruge en anmodning om tilladelse ved kørselstid, når dette er muligt, inden du får adgang til data, der er begrænset af [Android-tilladelser](#).
- Ikke sælge personlige eller følsomme brugerdata.

Krav om tydelig erklæring og samtykke

I tilfælde, hvor brugerne med rimelighed ikke forventer, at deres personlige eller følsomme brugerdata er nødvendige for at levere eller forbedre de funktioner i din app, der overholder politikkerne (f.eks. dataindsamling, der foregår i baggrunden i din app), skal du opfylde følgende krav:

Din app skal indeholde en erklæring om din adgang til, indsamling, brug og deling af data. Erklæringen i appen:

- Skal vises i selve appen, ikke kun i appbeskrivelsen eller på et website
- Skal vises ved normal brug af appen og ikke kræve, at brugeren går ind i en menu eller i indstillingerne
- Skal beskrive de data, der gives adgang til eller indsamles
- Skal forklare, hvordan dataene bruges og/eller deles
- **Må ikke** kun angives i en privatlivspolitik eller i servicevilkårene
- **Må ikke** inkluderes i andre erklæringer, der ikke har med indsamling af personlige eller følsomme oplysninger at gøre

Erklæringen i din app skal ledsage og gå umiddelbart forud for en anmodning om brugerens samtykke samt en tilknyttet tilladelse ved kørselstid, hvis den er tilgængelig. Du må ikke bruge eller indsamle personlige eller følsomme brugerdata, før brugeren har givet samtykke. Appens anmodning om samtykke:

- Skal klart og tydeligt vise dialogboksen til samtykke.
- Skal kræve en aktiv handling fra brugerens side (f.eks. et tryk for at acceptere eller markering af et afkrydsningsfelt).
- **Må ikke** tolke det som samtykke, at der navigeres væk fra meddelelsen, herunder at trykke væk eller trykke på knappen Tilbage eller Hjem.
- **Må ikke** benytte meddelelser, der lukker automatisk eller udløber, til at indhente brugersamtykke.

Her er nogle eksempler på typiske overtrædelser:

- En app, der har adgang til en brugers oversigt over installerede apps og ikke behandler disse data som personlige eller følsomme oplysninger i henhold til ovenstående krav om privatlivspolitik, databehandling, tydelig erklæring og tydeligt samtykke.
- En app, der har adgang til en brugers telefonbogsdata eller data om kontakter og ikke behandler disse data som personlige eller følsomme oplysninger i henhold til ovenstående krav om privatlivspolitik, databehandling, tydelig erklæring og tydeligt samtykke.
- En app, der registrerer en brugers skærm og ikke behandler disse data som personlige eller følsomme oplysninger i henhold til privatlivspolitikken.
- En app, der indsamler [enhedens placering](#) og ikke tydeligt oplyser om dens brug og indhenter samtykke i overensstemmelse med ovenstående krav
- En app, der indsamler begrænsede tilladelser i appens baggrund, herunder til sporing-, research- eller marketingformål, og ikke tydeligt oplyser om dens brug og indhenter samtykke i overensstemmelse med ovenstående krav.

Specifikke begrænsninger for adgang til følsomme data

Foruden ovennævnte krav beskriver tabellen nedenfor kravene for specifikke aktiviteter.

Aktivitet	Krav
Din app håndterer betalingsoplysninger eller andre økonomiske oplysninger eller personnumre	Din app må aldrig offentliggøre personlige eller følsomme brugerdata relateret til betalingsaktivitet, andre økonomiske aktiviteter eller eventuelle personnumre.
Din app håndterer ikke-offentlige oplysninger fra telefonbogen eller kontaktoplysninger	Vi tillader ikke uautoriseret offentliggørelse eller afsløring af folks ikke-offentlige kontakter.
Din app indeholder antivirus- eller sikkerhedsfunktionalitet som f.eks. antivirus-, antimalware- eller sikkerhedsrelaterede funktioner	Din app skal angive en privatlivspolitik, som sammen med alle erklæringer i appen forklarer, hvilke brugerdata din app indsamler og videregiver, hvad dataene skal bruges til, og hvilke grupper de deles med.

EU-U.S. Privacy Shield (Privacy Shield-principperne for transatlantiske dataudvekslinger)

Privacy Shield

Hvis du har adgang til, bruger eller behandler personlige oplysninger, som stilles til rådighed af Google, der direkte eller indirekte identificerer en person, og som stammer fra et EU-land eller Schweiz ("EU-personoplysninger"), skal du:

- Overholde alle gældende love, direktiver, forskrifter og regler for privatliv, datasikkerhed og databeskyttelse
- Kun have adgang til, bruge eller behandle EU-personoplysninger, der stemmer overens med det samtykke, som vedkommende, til hvem EU-personoplysningerne relaterer, har givet
- Implementere passende organisatoriske og tekniske foranstaltninger til beskyttelsen af EU-personoplysninger i forbindelse med tab, misbrug og uautoriseret eller ulovlig adgang, offentliggørelse, ændring og destruktion
- Levere det samme niveau af beskyttelse, som er påkrævet i henhold til [Privacy Shield-principperne](#).

Du skal regelmæssigt føre kontrol med, om du overholder disse betingelser. Hvis du på noget tidspunkt ikke kan overholde disse betingelser (eller hvis der er en betydelig risiko for, at du ikke kan overholde dem), skal du straks give os besked via mail på data-protection-office@google.com og øjeblikkeligt stoppe med at behandle EU-personoplysninger eller på en rimelig og hensigtsmæssig måde genoprette et acceptabelt sikkerhedsniveau.

Tilladelser

Anmodninger om tilladelse skal give mening for brugerne. Du må kun anmode om tilladelser, som er nødvendige for at implementere eksisterende funktioner eller tjenester i din app, der promoveres på din profilside i Play Butik. Du må ikke bruge tilladelser, der giver adgang til bruger- eller enhedsdata med henblik på ikke-oplyste, ikke-implementerede eller ikke-tilladte funktioner eller formål. Personlige eller følsomme data, der gives adgang til via tilladelser, må aldrig sælges.

Anmod om tilladelser for at få adgang til data i den rette sammenhæng (via trinvis godkendelse), så brugerne forstår, hvorfor din app anmoder om tilladelsen. Brug kun dataene til formål, som brugeren har givet sit samtykke til. Hvis du senere ønsker at bruge dataene til andre formål, skal du spørge brugerne og sørge for, at de giver bekræftende samtykke til den yderligere brug.

Begrænsede tilladelser

Begrænsede tilladelser er, ud over ovenstående, tilladelser, der er angivet som [Farlig](#), [Særlig](#) eller [Signatur](#), og er underlagt følgende yderligere krav og begrænsninger:

- Følsomme bruger- eller enhedsoplysninger, som du får adgang til via begrænsede tilladelser, må kun overføres til tredjeparter, hvis det er nødvendigt for at levere eller forbedre eksisterende funktioner eller tjenester i den app, hvorfra dataene blev indsamlet. Du må også overføre data, hvis det er nødvendigt for at overholde gældende lovgivning eller i forbindelse med en fusion, et opkøb eller et salg af aktiver med juridisk tilstrækkeligt varsel til brugerne. Alle andre overførsler eller salg af brugerdata er forbudt.
- Respekter brugernes beslutninger, hvis de afviser en anmodning om en begrænset tilladelse. Brugerne må ikke manipuleres eller tvinges til at give samtykke til ikke-kritiske tilladelser. Du skal gøre et rimeligt forsøg på at imødekomme brugere, der ikke giver adgang til følsomme tilladelser (f.eks. give brugeren mulighed for at angive et telefonnummer manuelt, hvis vedkommende har begrænset adgangen til Opkaldsliste).

Visse begrænsede tilladelser kan være underlagt yderligere krav som beskrevet nedenfor. Formålet med disse begrænsninger er at beskytte brugernes personlige oplysninger. Vi kan gøre begrænsede undtagelser til nedenstående krav i meget sjældne tilfælde, hvor apps leverer en særdeles interessant eller kritisk funktion, og hvor der ikke findes alternative metoder til at levere funktionen. Vi evaluerer foreslåede undtagelser i forhold til den potentielle påvirkning af brugernes privatliv eller sikkerhed.

Tilladelser til sms- og opkaldsliste

Tilladelser til sms- og opkaldsliste anses som personlige og følsomme brugerdata, der er underlagt politikken om [personlige og følsomme oplysninger](#) og følgende begrænsninger:

Begrænset tilladelse	Krav
Dit appmanifest anmoder om tilladelsesgruppen Opkaldsliste (f.eks. <code>READ_CALL_LOG</code> , <code>WRITE_CALL_LOG</code> , <code>PROCESS_OUTGOING_CALLS</code>)	Den skal være aktivt registreret som standardprogram for telefon eller Assistent på enheden.
Dit appmanifest anmoder om tilladelsesgruppen Sms (f.eks. <code>READ_SMS</code> , <code>SEND_SMS</code> , <code>WRITE_SMS</code> , <code>RECEIVE_SMS</code> , <code>RECEIVE_WAP_PUSH</code> , <code>RECEIVE_MMS</code>)	Den skal være aktivt registreret som standardprogram til sms eller Assistent på enheden.

Apps, der ikke kan være standardprogram til sms, opkald eller Assistent, må ikke angive brug af ovenstående tilladelser i manifestet. Dette gælder også pladsholdertekst i manifestet. Apps skal desuden være aktivt registreret som standardprogram for sms, telefon eller Assistent, inden de anmoder brugere om at acceptere nogen af ovenstående tilladelser, og de skal straks stoppe med at bruge tilladelserne, når de ikke længere fungerer som standardprogram. De tilladte anvendelser og undtagelser kan findes på [denne side i Hjælp](#).

Apps må kun bruge tilladelsen (og data, der er afledt af tilladelsen) til at levere godkendt kernefunktionalitet for appen. Kernefunktionalitet defineres som hovedformålet med appen. Dette kan omfatte en række primære funktioner, som alle skal være dokumenteret og promoveret i appens beskrivelse. Uden kernefunktionen er appen "defekt" eller ubrugelig. Overførsel, deling eller licenseret brug af disse data må kun ske med henblik på at levere kernefunktioner eller tjenester i appen, og brugen heraf må ikke udvides til andre formål (f.eks. forbedring af andre apps eller tjenester, reklame eller markedsføring). Du må ikke bruge alternative metoder (herunder andre tilladelser, API'er eller tredjepartskilder) til at udlede data, der er tilskrevet tilladelserne Opkaldsliste eller Sms.

Adgangstilladelser til placering

[Enhedsplacering](#) anses som personlige og følsomme brugerdata, der er underlagt politikken om [personlige og følsomme oplysninger](#) og følgende krav:

- Apps må ikke have adgang til data, der beskyttes af adgangstilladelser til placering (f.eks. `ACCESS_FINE_LOCATION`, `ACCESS_COARSE_LOCATION`, `ACCESS_BACKGROUND_LOCATION`), når de ikke længere er nødvendige for at levere eksisterende funktioner eller tjenester i din app.
- Du bør aldrig anmode brugere om adgangstilladelser til placering udelukkende med henblik på annoncering eller dataanalyse. Apps, der udvider den tilladte brug af disse data til annoncevisning, skal overholde vores [annoncepolitik](#).
- Apps skal anmode om det laveste omfang, der er nødvendigt (dvs. omtrentligt i stedet for nøjagtigt og forgrund i stedet for baggrund) for at levere den eksisterende funktion eller tjeneste, der kræver oplysninger om placeringen, og brugere bør med rimelighed forvente, at funktionen eller tjenesten har brug for det placeringsniveau, der anmodes om. Vi kan f.eks. afvise apps, der anmoder om eller har adgang til baggrundsplacering uden overbevisende begrundelse.
- Placering i baggrunden må kun bruges til at levere funktioner, der er til gavn for brugeren og relevante for appens kernefunktionalitet.

Apps har adgangstilladelse til placering ved hjælp af tjenesten i forgrunden (når appen kun har adgang i forgrunden, f.eks. "mens den er i brug"), hvis brugen:

- Er påbegyndt som en fortsættelse af en handling, som brugeren har påbegyndt i appen.
- Afsluttes, straks efter den tiltænkte brug af den brugerindledte handling er udført af appen.

Apps, der er udviklet specielt til børn, skal overholde politikken [For hele familien](#).

Adgangstilladelse til alle filer

Filer og mappeattributter på en brugers enhed betragtes som personlige og følsomme brugerdata, der er underlagt politikken om [personlige og følsomme oplysninger](#) og følgende krav:

- Apps må kun anmode om adgang til enhedens lagerplads i det omfang, det er nødvendigt for, at appen kan fungere, og må ikke anmode om adgang til enhedens lager på vegne af tredjeparter til noget formål, der ikke er relateret til vigtige brugerrettede appfunktioner.
- Android-enheder, der kører R (Android 11, API-niveau 30) eller nyere, kræver tilladelsen [MANAGE_EXTERNAL_STORAGE](#) for at administrere adgangen til delt hukommelse. Alle apps, der er målrettet mod R og anmoder om bred adgang til delt hukommelse ("Adgang til alle filer"), skal bestå en passende adgangsgennemgang inden udgivelse. Apps, der må anvende denne tilladelse, skal tydeligt bede brugerne om at aktivere "Adgang til alle filer" for deres app under indstillingerne for "Særlig appadgang". Du kan få flere oplysninger om R-kravene i denne artikel i Hjælp.

Enheds- og netværksmisbrug

Vi tillader ikke apps, der forstyrrer, afbryder, beskadiger eller opnår uautoriseret adgang til brugerens enhed, andre enheder eller computere, servere, netværk, API'er eller tjenester, herunder, men ikke begrænset til, andre apps på enheden, en Google-tjeneste eller et netværk tilhørende et autoriseret mobilselskab.

Apps i Google Play skal overholde Androids standardkrav til systemoptimering, som er beskrevet i de [centrale retningslinjer for appkvalitet i Google Play](#).

En app, der distribueres via Google Play, må ikke modificere, erstatte eller opdatere sig selv ved hjælp af andre metoder end Google Plays opdateringsmekanisme. På samme måde må en app heller ikke downloade eksekverbar kode (f.eks. dex-, JAR- eller .so-filer) fra en anden kilde end Google Play. Denne begrænsning gælder ikke for kode, der kører i en virtuel maskine, og som har begrænset adgang til Android API'er (f.eks. JavaScript i en webvisning eller en browser).

Vi tillader ikke kode, der introducerer eller udnytter sikkerhedsbrister. Se siden om [Sikkerhedsoptimering for apps](#) for at få oplysninger om de nyeste sikkerhedsproblemer, som er rapporteret til udviklere i Google Play.

Her er nogle eksempler på typiske overtrædelser:

- Apps, der blokerer eller forstyrrer en anden apps annoncevisning.
- Apps med snydekoder til spil, som påvirker gameplay i andre apps.
- Apps, som muliggør eller indeholder vejledninger i, hvordan man hacker tjenester, software eller hardware, eller hvordan man omgår sikkerhedsforanstaltninger.
- Apps, der får adgang til eller bruger en tjeneste eller API på en måde, som overtræder dens servicevilkår.
- Apps, der ikke er [kvalificeret til hvidlister](#) og forsøger at omgå [systemets strømstyring](#).
- Apps, der faciliterer proxytjenester til tredjeparter, må kun gøre det i apps, hvor dette er det primære hovedformål for brugeren af appen.
- Apps eller tredjepartskode (f.eks. SDK'er), der downloader eksekverbar kode, f.eks. dex-filer eller oprindelig kode, fra en anden kilde end Google Play.
- Apps, der installerer andre apps på en enhed uden forudgående samtykke fra brugeren.
- Apps, der linker til eller assisterer med distribution eller installation af skadelig software.

Vildledende adfærd

Vi tillader ikke apps, der forsøger at vildlede brugerne eller muliggør bedragerisk adfærd. Dette inkluderer, men er ikke begrænset til, apps, som vi vurderer til at være funktionelt umulige. Apps skal give nøjagtige oplysninger, beskrivelser og billeder/video af deres funktionalitet i alle metadata. Apps må heller ikke efterligne funktionalitet eller advarsler fra operativsystemet eller andre apps. Enhedsindstillingerne må kun ændres med brugerens kendskab og samtykke, og brugeren skal kunne fortryde ændringerne.

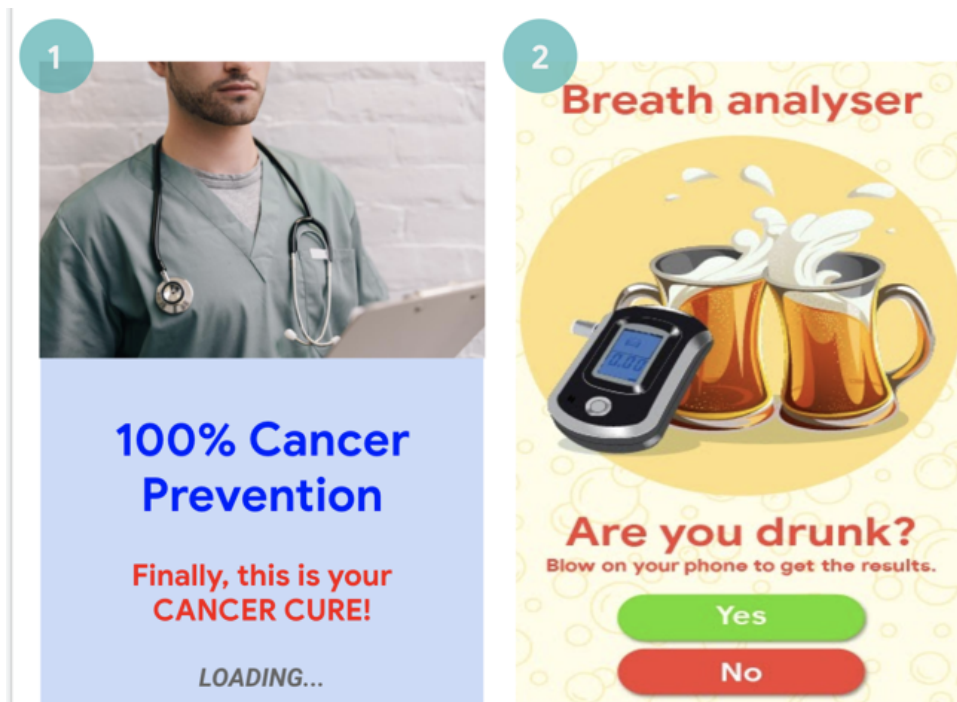
Vildledende påstande

Vi tillader ikke apps, der indeholder falske eller vildledende oplysninger eller påstande i beskrivelsen, navnet, ikonet eller på screenshots.

Her er nogle eksempler på typiske overtrædelser:

- Apps, der indeholder en misvisende, unøjagtig eller tvetydig beskrivelse af funktionaliteten:
 - En app, der i henhold til beskrivelsen og screenshots ser ud til at være et bilspil, men som i virkeligheden er et puslespil med et billede af en bil.
 - En app, der udgiver sig for at være en antivirusapp, men som kun indeholder en tekstvejledning i, hvordan man fjerner virus.
- Udvikler- eller appnavne, der indeholder misvisende oplysninger om deres nuværende status eller effektivitet i Play. (Det kunne f.eks. være "Redaktørens udvalgte", "App nummer 1", "Mest populære betalte").
- Apps, der indeholder lægelige eller sundhedsrelaterede funktioner, som er misvisende eller potentielt skadelige.

- Apps, som påstås at indeholde funktioner, der ikke er mulige for brugeren at implementere (f.eks. apps, der påstår, at de jager insekter væk), selv hvis påstanden præsenteres som en spøg, en forfalskning, en vittighed el.lign.
- Apps, der er forkert kategoriseret, herunder, men ikke begrænset til, appens klassificering eller kategori.
- Påviseligt vildledende indhold, der kan påvirke afstemninger.
- Apps, der på et falsk grundlag hævder at være tilknyttet en offentlig myndighed eller levere eller muliggøre offentlige tjenester, som de ikke er autoriseret til at udføre.
- Apps, som fejlagtigt påstår at være den officielle app for en etableret juridisk part. Navne som f.eks. "Justin Bieber Official" er ikke tilladt uden de nødvendige tilladelser eller rettigheder.



- (1) Denne app indeholder medicinske eller sundhedsrelaterede påstande (kurerer kræft), der er vildledende
 (2) Denne app påstår at have funktioner, der ikke er mulige at implementere (brug af din telefon som et alkometer)

Vildledende ændringer af enhedsindstillingerne

Vi tillader ikke apps, der foretager ændringer af brugerens enhedsindstillinger eller -funktioner uden for appen uden brugerens kendskab og samtykke. Enhedsindstillinger og -funktioner omfatter system- og browserindstillinger, bogmærker, genveje, ikoner, widgets og præsentationen af apps på startskærmen.

Vi tillader desuden ikke:

- Apps, der ændrer enhedsindstillinger og -funktioner med brugerens samtykke, men som gør det på en måde, så ændringerne ikke nemt kan fortrydes.
- Apps eller annoncer, der ændrer enhedsindstillinger eller -funktioner som en tjeneste for tredjeparter eller til markedsføringsformål.
- Apps, der vildleder brugerne til at fjerne eller deaktivere apps fra tredjeparter eller ændre enhedsindstillinger eller -funktioner.
- Apps, der opfordrer brugerne eller giver dem incitamenter til at fjerne eller deaktivere tredjepartsapps eller ændre enhedsindstillinger eller -funktioner, medmindre det er som en del af en verificerbar sikkerhedstjeneste.

Muliggørelse af bedragerisk adfærd

Vi tillader ikke apps, der hjælper brugerne med at vildlede andre, eller som er funktionelt vildledende på nogen måde, herunder, men ikke begrænset til, apps, som genererer eller muliggør generering af id-kort, cpr-numre, pas, eksamensbeviser, betalingskort og kørekort. Apps skal give nøjagtige oplysninger, titler, beskrivelser og billeder/video vedrørende appens funktion og/eller indhold, og de skal fungere, som brugeren med rimelighed og nøjagtighed forventer.

Yderligere appressourer (f.eks. spilaktiver) må kun downloades, hvis de er nødvendige for, at brugeren kan anvende appen. Downloadede ressourcer skal overholde alle Google Play-politikker, og brugerne skal have mulighed for at give tilladelse, inden downloaden går i gang. Størrelsen på downloaden skal desuden fremgå tydeligt.

Påstande om, at en app er "for sjov", "kun til underholdning" (eller andre synonymer), fritager ikke en app fra at overholde vores politikker.

Her er nogle eksempler på typiske overtrædelser:

- Apps, der efterligner andre apps eller websites for at narre brugerne til at videregive personlige oplysninger eller godkendelsesoplysninger.
- Apps, der afbilder eller viser ubekræftede eller virkelige telefonnumre, kontakter, adresser eller personhenførbare oplysninger for enkeltpersoner eller enheder, der ikke har givet samtykke.
- Apps med forskellige kernefunktioner, der er baseret på en brugers geografi, enhedsparametre eller andre brugerafhængige data, hvor disse forskelle ikke oplyses tydeligt til brugeren på profilsiden i Play Butik.
- Apps, der ændres væsentligt fra den ene version til den anden uden at underrette brugeren (f.eks. i [sektionen "Nyheder"](#)) eller opdatere profilsiden i Play Butik.
- Apps, der forsøger at ændre eller sløre adfærd under gennemgangen.
- Apps med downloads via netværk til indholdslevering (CDN, content delivery network), som ikke anmoder om brugerens tilladelse og ikke oplyser størrelsen på downloaden, inden den går i gang.

Manipulerede medier

Vi tillader ikke apps, der promoverer eller hjælper med at oprette falske eller vildledende oplysninger eller påstande, der formidles via billeder, videoer og/eller tekst. Vi tillader ikke apps, som vi vurderer promoverer eller udbreder bevisligt misvisende eller vildledende billeder, videoer og/eller tekst, som kan forvolde skade i forbindelse med en følsom begivenhed, politik, sociale problemer eller andre sager af offentlig interesse.

Apps, der manipulerer med eller ændrer medier ud over konventionelle og redaktionelt accepterbare justeringer med henblik på nøjagtighed eller kvalitet, skal tydeligt oplyse om eller vandmærke ændrede medier, når det muligvis ikke fremgår klart for en gennemsnitlig bruger, at mediet er blevet ændret. Der kan gøres undtagelser, hvis det vurderes at være af offentlig interesse eller ved åbenlys satire eller parodi.

Her er nogle eksempler på typiske overtrædelser:

- Apps, der knytter en offentlig person til en demonstration ved en politisk følsom begivenhed.
- Apps, der bruger offentlige personer eller medier fra en følsom begivenhed til at reklamere for en funktion, der kan ændre medier, på en apps profilside i Play Butik.
- Apps, der ændrer medieklip for at efterligne en nyhedsudsendelse.



(1) Denne app har funktioner til at ændre medieklip, så de efterligner en nyhedsudsendelse, og tilføje kendte eller offentlige personer til klippet uden at tilføje et vandmærke.

Urigtige oplysninger

Vi tillader ikke apps eller udviklerkonti, der:

- Udgiver sig for at være en anden person eller organisation, eller som fordrejer eller skjuler deres ejerskab eller primære formål.
- Deltager i koordinerede aktiviteter med henblik på at vildlede brugerne. Dette omfatter, men er ikke begrænset til, apps og udviklerkonti, der giver urigtige oplysninger om, hvilket land de stammer fra, eller som sender indhold til brugere i et andet land.
- Koordinerer med andre apps, websites, udviklere eller andre konti for at skjule eller give urigtige oplysninger om udvikler- eller appidentitet eller andre væsentlige detaljer, hvor appindholdet omhandler politik eller sociale emner, som har offentlig interesse.

Malware

Malware er enhver form for kode, der kan udsætte en bruger, en brugers data eller en enhed for fare. Malware omfatter, men er ikke begrænset til, potentielt skadelige apps, binære programmer eller systemændringer, der falder ind under kategorier som trojanske heste, phishing og spywareapps, og vi opdaterer og tilføjer løbende nye kategorier.

Malware

Vores politik vedrørende malware er enkel: Android-økosystemet, herunder Google Play Butik, og brugernes enheder skal beskyttes helt og holdent mod skadelig adfærd (dvs. malware). Ud fra dette grundlæggende princip bestræber vi os på at levere et Android-økosystem, der er sikkert for vores brugere og deres Android-enheder.

Malware kan variere alt efter type og funktion, men har typisk et af følgende formål:

- At kompromittere integriteten af brugerens enhed.
- At overtage kontrollen af en brugers enhed.
- At aktivere fjernstyrede processer, hvormed en hacker kan få adgang til, bruge eller på anden måde udnytte en inficeret enhed.
- At overføre personoplysninger eller loginoplysninger fra enheden uden tilstrækkelige oplysninger og samtykke.
- At sende spam eller kommandoer fra den inficerede enhed for at ramme andre enheder eller netværk.
- At bedrage brugeren.

En app, et binært program eller en systemændring kan potentielt være skadelig og kan derfor medføre ondsindet adfærd, selv om det ikke var hensigten. Dette skyldes, at apps, binære programmer eller systemændringer kan fungere forskelligt afhængigt af en række variabler. Det, der er skadeligt for én Android-enhed, udgør derfor ikke nødvendigvis en risiko for en anden Android-enhed. En enhed med den nyeste version af Android påvirkes f.eks. ikke af skadelige apps, der bruger forældede API'er til at udføre ondsindet adfærd, mens en enhed, som stadig har en meget gammel version af Android, kan være i risikogruppen. Apps, binære programmer eller systemændringer betragtes som malware eller potentielt skadelige apps, hvis de udgør en klar risiko for nogle eller alle Android-enheder og -brugere.

Malwarekategorierne nedenfor afspejler vores grundlæggende tro på, at brugerne bør forstå, hvordan deres enhed kan udnyttes, og promoverer et sikkert økosystem, der fremmer effektiv innovation og en brugeroplevelse, der er tillid til.

Gå til [Google Play Protect](#) for at få flere oplysninger.

Bagdøre

Kode, der gør det muligt at udføre uønskede, potentielt skadelige fjernstyrede processer på en enhed.

Disse processer kan omfatte adfærd, som kan placere appen, det binære program eller systemændringen i en af de andre malwarekategorier, hvis de udføres automatisk. En "bagdør" er generelt en beskrivelse af, hvordan en potentielt skadelig proces kan opstå på en enhed, og er derfor ikke helt på linje med kategorier som faktureringsbedrageri eller kommerciel spyware. Af denne årsag behandler Google Play Protect under visse omstændigheder nogle bagdøre som sårbarheder.

Faktureringsbedrageri

Kode, der automatisk debiterer brugeren på en bevidst vildledende måde.

Bedrageri i forbindelse med mobilfakturering kan opdeles i sms-bedrageri, opkaldsbedrageri og afgiftsbedrageri.

Sms-svind

Kode, der debiterer brugere for at sende en overtaget sms-besked uden samtykke, eller som forsøger at camouflere sine sms-aktiviteter ved at skjule brugsvilkår eller sms-beskeder fra mobilselskabet, der underretter brugeren om opkrævninger eller bekræfter abonnementer.

Noget kode introducerer yderligere adfærd, der faciliterer sms-bedrageri, selvom de teknisk set afslører afsendelsesadfærd. Eksempler på dette omfatter, at dele af brugsvilkårene skjules for brugeren, at indhold gøres ulæseligt, og at sms-beskeder fra mobilselskabet, der informerer brugeren om opkrævninger eller bekræfter et abonnement, undertrykkes under visse betingelser.

Opkaldssvind

Kode, der debiterer brugere ved at foretage opkald til overtakserede numre uden brugerens samtykke.

Gebyrsvind

Kode, der narrer brugere til at abonnere på eller købe indhold via deres mobilregning.

Afgiftsbedrageri omfatter enhver type fakturering med undtagelse af overtakserede sms-beskeder og opkald. Eksempler på dette omfatter betaling via mobilregningen, trådløst adgangspunkt og overførsel af mobilsendetid. Bedrageri med trådløst adgangspunkt er en af de mest udbredte typer afgiftsbedrageri. Bedrageri med trådløst adgangspunkt kan omfatte, at brugere narres til at klikke på en knap i en gennemsigtig webvisning, der indlæses lydløst. Når handlingen er udført, startes et fast abonnement, og den sms-besked eller mail, der sendes som bekræftelse, kapres ofte for at forhindre brugere i at opdage den finansielle transaktion.

Stalkerware

Kode, der sender personlige oplysninger fra enheden uden tilstrækkelig varsel eller samtykke, og som ikke viser en vedvarende notifikation om, at dette finder sted.

Stalkerware-apps sender typisk data til en anden part end udbyderen af den potentielt skadelige app.

Accepterede versioner af disse apps kan bruges af forældre til at spore deres børn. Disse apps kan dog ikke bruges til at spore en person (f.eks. en ægtefælle) uden dennes kendskab eller tilladelse, medmindre der vises en vedvarende notifikation, mens dataene overføres.

Kun apps, der overholder politikkerne, og som udelukkende er designet og markedsført til forældres (herunder familiers) opsyn eller virksomheders administration, må distribueres i Play Butik med sporings- og rapporteringsfunktioner, forudsat at de fuldt ud opfylder de krav, der er beskrevet nedenfor.

Stalkerwarefrie apps, der distribueres i Play Butik, og som overvåger eller sporer en brugers adfærd på en enhed, skal overholde følgende krav:

- Apps må ikke udgive sig for at være et værktøj til spionage eller hemmelig overvågning.
- Apps må ikke skjule eller tilsløre sporingsadfærd eller forsøge at vildlede brugere i forbindelse med en sådan funktionalitet.
- Apps skal give brugerne en vedvarende notifikation og et unikt ikon, som tydeligt identificerer appen.
- Apps og appfortegnelser i Google Play må ikke angive nogen metoder, der aktiverer eller giver adgang til funktionaliteter, som overtræder disse vilkår, f.eks. et link til en APK-fil, der ikke opfylder kravene, og som hostes uden for Google Play.
- Du alene er ansvarlig for at afgøre, om din app er lovlig i det område, du målretter den mod. Apps, som viser sig at være ulovlige i områder, hvor de er udgivet, bliver fjernet.

Denial of Service (DoS)

Kode, der udfører et DoS-angreb (Denial of Service), eller som er en del af et DDoS-angreb (Distributed Denial of Service) mod andre systemer og ressourcer.

Det kan f.eks. udføres ved at sende et stort antal HTTP-anmodninger for at lægge overdrevent pres på eksterne servere.

Skadelige downloadprogrammer

Kode, der ikke i sig selv er potentielt skadelig, men som downloader andre potentielt skadelige apps.

Kode kan være et skadeligt downloadprogram, hvis:

- Der er grund til at tro, at den blev udviklet med henblik på at sprede potentielt skadelige apps, og den har downloadet potentielt skadelige apps eller indeholder kode, der kan downloade og installere apps.
- Mindst 5 % af apps, som downloades af den, er potentielt skadelige apps med en mindstegrænse på 500 observerede appdownloads (25 observerede downloads af potentielt skadelige apps).

Populære browsere og apps til fildeling betragtes ikke som skadelige downloadprogrammer, så længe følgende er gældende:

- De starter ikke downloads uden brugerens interaktion.
- Alle downloads af potentielt skadelige apps startes efter brugerens samtykke.

Trussel mod andre systemer end Android

Kode, som indeholder trusler mod andre systemer end Android.

Disse apps kan ikke skade Android-brugeren eller -enheden, men indeholder komponenter, der potentielt kan skade andre platforme.

Phishing

Kode, der foregiver at komme fra en troværdig kilde, anmoder om en brugers godkendelses- eller faktureringsoplysninger og sender disse data til en tredjepart. Denne kategori gælder også for kode, der opsnapper brugeroplysninger under overførslen.

Phishing er typisk målrettet mod bankoplysninger, kreditkortnumre og loginoplysninger til onlinekonti på sociale netværk og til spil.

Misbrug af rettigheder til integrerede apps

Kode, der kompromitterer systemets integritet ved at bryde ud af appens sandbox, opnå rettigheder til integrerede apps eller ændre eller deaktivere adgang til vigtige sikkerhedsrelaterede funktioner.

Eksempler:

- En app, der overtræder tilladelsesmodellen for Android eller stjæler loginoplysninger (f.eks. OAuth-token) fra andre apps.
- Apps, der misbruger funktioner for at forhindre, at de bliver afinstalleret eller standset.
- En app, der deaktiverer SELinux.

Apps til eskalering af rettigheder, der rooter enheder uden brugerens tilladelse, klassificeres om rootingapps.

Ransomware

Kode, der tager delvis eller omfattende kontrol over en enhed eller data på en enhed og forlanger, at brugeren betaler eller udfører en handling for at få kontrollen tilbage.

Noget ransomware krypterer data på enheden og forlanger betaling for at afkryptere de pågældende data og/eller udnytter enhedens administratorfunktioner, så det ikke kan fjernes af en typisk bruger. Eksempler:

- Låse en bruger ude fra enheden og forlange penge for at give brugeren kontrollen tilbage.
- Kryptere data på enheden og forlange betaling angiveligt for at afkryptere dataene.
- Udnytte funktioner til administration af enhedspolitikker og forhindre brugeren i at fjerne appen.

Kode, der distribueres med enheden, hvis primære formål er subsidieret enhedsadministration, kan fjernes fra ransomwarekategorien, forudsat at den opfylder kravene for sikker låsning og administration samt kravene om tilstrækkelig oplysning til og samtykke fra brugeren.

Rooting

Kode, der rooter enheden.

Der er forskel på ikke-skadelig og skadelig rootingkode. Ikke-skadelige rootingapps giver f.eks. brugeren forudgående besked om, at de rooter enheden, og de udfører ikke andre potentielt skadelige handlinger, der er kendt fra andre kategorier af potentielt skadelige apps.

Skadelige rootingapps informerer ikke brugeren om, at de rooter enheden, eller også informerer de brugeren om en rooting, inden den udføres, men de udfører også andre handlinger, der er kendt fra andre kategorier af potentielt skadelige apps.

Spam

Kode, der sender uopfordrede beskeder til brugernes kontakter eller bruger enheden til videresendelse af spammail.

Spyware

Kode, der sender personoplysninger fra enheden uden tilstrækkeligt varsel eller samtykke.

For at det kan anses som spyware, er det f.eks. tilstrækkeligt, at nogle af følgende oplysninger sendes uden at gøre opmærksom på det eller på en måde, som brugeren ikke forventer:

- Liste over kontakter
- Billeder eller andre filer fra SD-kortet, eller som ikke ejes af appen
- Indhold fra brugermails
- Opkaldsliste
- Sms-liste
- Webhistorik eller bogmærker fra standardbrowseren
- Information fra /data/-mapper, der tilhører andre apps.

Adfærd, der kan anses som udspionering af brugeren, kan også rapporteres som spyware. Dette kan f.eks. være optagelse af lyd eller optagelse af opkald, der modtages på telefonen, eller tyveri af appdata.

Trojansk hest

Kode, der tilsyneladende er uskadelig, f.eks. et spil, der giver sig ud for kun at være et spil, men som udfører uønskede processer til skade for brugeren.

Denne klassificering bruges normalt i kombination med andre kategorier af potentielt skadelige apps. En trojansk hest har en harmløs komponent og en skjult skadelig komponent. Det kan f.eks. være et spil, der sender overtakserede sms-beskeder fra brugerens enhed i baggrunden og uden brugerens viden.

En bemærkning vedrørende atypiske apps

Nye og usædvanlige apps kan klassificeres som atypiske, hvis Google Play Protect ikke har tilstrækkelig information til at erklære dem for sikre. Det betyder ikke, at appen nødvendigvis er skadelig, men uden yderligere gennemgang kan den heller ikke erklæres for sikker.

En bemærkning om kategorien Bagdør

Klassificering som malwarekategorien "bagdør" afhænger af, hvordan koden opfører sig. Hvis kode skal klassificeres som bagdørsmalware, er det en nødvendig betingelse, at den muliggør adfærd, som ville placere koden i en af de andre malwarekategorier, hvis den udføres automatisk. Hvis en app f.eks. tillader dynamisk indlæsning af kode, og den dynamisk indlæste kode henter sms-beskeder, klassificeres den som bagdørsmalware.

Hvis en app tillader udførelse af vilkårlig kode, og vi ikke har grund til at tro, at denne funktion er tilføjet med henblik på skadelig adfærd, vil appen dog blive behandlet som en app med en sårbarhed i stedet for bagdørsmalware, og udvikleren bliver bedt om at rette den.

Uønsket software til mobilenheder

Denne politik udbygger Googles politik om uønsket software ved at opridse principperne for Android-økosystemet og Google Play Butik. Software, der overtræder disse principper, kan være skadelig for brugeroplevelsen, og vi træffer foranstaltninger for at beskytte brugerne mod den.

Uønsket software til mobilenheder

Hos Google arbejder vi ud fra den overbevisning, at hvis vi fokuserer på brugeren, kommer resten af sig selv. I vores [softwareprincipper](#) og [politikken om uønsket software](#) giver vi generelle anbefalinger til software, der giver en god brugeroplevelse. Denne politik udbygger Googles politik om uønsket software ved at opridse principperne for Android-økosystemet og Google Play Butik. Software, der overtræder disse principper, kan være skadelig for brugeroplevelsen, og vi træffer foranstaltninger for at beskytte brugerne mod den.

Som nævnt i [politikken om uønsket software](#) har vi konstateret, at uønsket software i de fleste tilfælde har en eller flere af de samme grundlæggende egenskaber:

- Den er vildledende og giver lovning på et værditilbud, den ikke opfylder.
- Den forsøger at narre brugerne til at installere den eller skjuler sig i installationsfilerne til et andet program.
- Den fortæller ikke brugeren om alle dens primære og væsentligste funktioner.
- Den påvirker brugerens system på uventede måder.
- Den indsamler eller overfører personlige oplysninger uden brugerens viden.

- Den indsamler eller overfører personlige oplysninger uden sikker håndtering (f.eks. overførsel via HTTPS)
- Den følger med anden software, og dens tilstedeværelse er ikke oplyst.

På mobilenheder er software kode i form af en app, binær kode, systemændring osv. For at forhindre software, der er skadelig for softwarens økosystem eller forstyrrer brugeroplevelsen, skrider vi til handling over for kode, der overtræder disse principper.

Nedenfor udbygger vi politikken om uønsket software for at udvide dens anvendelighed til mobilsoftware. På samme måde som med denne politik fortsætter vi med at justere politikken om uønsket software til mobilenheder for at tage hånd om nye typer misbrug.

Gennemsigtig adfærd og tydelige erklæringer

Al kode skal indfri de løfter, der gives til brugeren. Apps skal levere alle funktioner, der oplyses i kommunikationen om appen. Apps må ikke forvirre brugerne.

- Apps skal tydeligt oplyse funktionalitet og formål.
- Forklar brugeren klart og tydeligt, hvilke systemændringer der foretages af appen. Giv brugerne mulighed for at gennemgå og godkende alle vigtige valgmuligheder og ændringer i forbindelse med installation af appen.
- Softwaren må ikke give urigtige oplysninger om tilstanden af brugerens enhed, f.eks. ved at påstå, at der er alvorlige sikkerhedsproblemer i systemet, eller at enheden er inficeret med virus.
- Brug ikke ugyldig aktivitet, der har til formål at øge annoncetrafikken og/eller antallet af konverteringer.
- Vi tillader ikke apps, der vildleder brugerne ved at efterligne andre (f.eks. en anden udvikler, virksomhed eller enhed) eller en anden app. Antyd ikke, at din app er relateret til eller godkendt af nogen, hvis det ikke er tilfældet.

Eksempler på overtrædelser:

- Annoncebedrageri
- Efterligning

Beskyt brugerdata

Vær tydelig og gennemsigtig i forhold til adgang, brug, indsamling og deling af personlige og følsomme brugerdata. Anvendelsen af brugerdata skal overholde alle relevante politikker for brugerdata, hvor det er relevant, og træffe alle forholdsregler for at beskytte dataene.

- Giv brugerne mulighed for at acceptere indsamlingen af deres data, før du begynder at indsamle og sende data fra enheden, herunder data om tredjepartskonti, mail, telefonnummer, installerede apps, filer, placering og andre personlige og følsomme data, som brugeren ikke forventer bliver indsamlet.
- De indsamlede personlige og følsomme brugerdata skal håndteres sikkert, herunder overføres ved hjælp af moderne kryptografi (f.eks. via HTTPS).
- Software, herunder mobilapps, må kun overføre personlige og følsomme brugerdata til servere, når dataene er relateret til appens funktionalitet.

Eksempler på overtrædelser:

- Dataindsamling (jf. [spyware](#))
- Misbrug af begrænsede tilladelser

Eksempler på brugerdatapolitikker:

- [Brugerdatapolitik i Google Play](#)
- [GMS-krav i brugerdatapolitikken](#)
- [Brugerdatapolitik for Google API-tjenesten](#)

Undgå forringelse af mobiloplevelsen

Brugeroplevelsen skal være ligetil, letforståelig og baseret på klare valg fra brugeren. Den skal give brugeren et klart værditilbud og må ikke forstyrre den annoncerede eller ønskede brugeroplevelse.

- Kør ikke annoncer, der vises til brugerne på uventede måder, f.eks. en visning, der forringer eller forstyrrer brugervenligheden af enhedens funktioner eller en visning uden for triggerappens miljø, hvis annoncen ikke er let at afvise, eller der ikke i tilstrækkelig grad angives samtykke og tilskrivning.
- Apps må ikke forstyrre andre apps eller enhedens anvendelighed
- Muligheden for at afinstallere skal vises tydeligt, hvor dette er relevant.
- Mobilsoftware må ikke efterligne meddelelser fra enhedens operativsystem eller andre apps. Du må ikke tilsidesætte underretninger til brugeren fra andre apps eller fra operativsystemet. Det gælder især underretninger til brugeren om, at der foretages ændringer i operativsystemet.

Eksempler på overtrædelser:

- Forstyrrende annoncer
- Uautoriseret brug eller efterligning af systemfunktioner

Annoncebedrageri

Annoncebedrageri er strengt forbudt. Annonceinteraktioner, der genereres med det formål at narre et annoncenetværk til at tro, at trafikken kommer fra autentisk brugerinteresse, udgør annoncebedrageri som en form for [ugyldig trafik](#).

Annoncebedrageri kan skyldes, at udviklere implementerer annoncer på ikke-tilladte måder, f.eks. ved at vise skjulte annoncer, automatisk klikke på annoncer, ændre oplysninger og på anden måde udnytte ikke-menneskelige handlinger (spiders, bots osv.) eller menneskelig aktivitet, der er beregnet til at generere ugyldige annoncetraфик. Ugyldig trafik og annoncebedrageri er skadelig for annoncører, udviklere og brugere og fører til langsigtet tab af tillid til økosystemet for mobilannoncer.

Her er nogle eksempler på typiske overtrædelser:

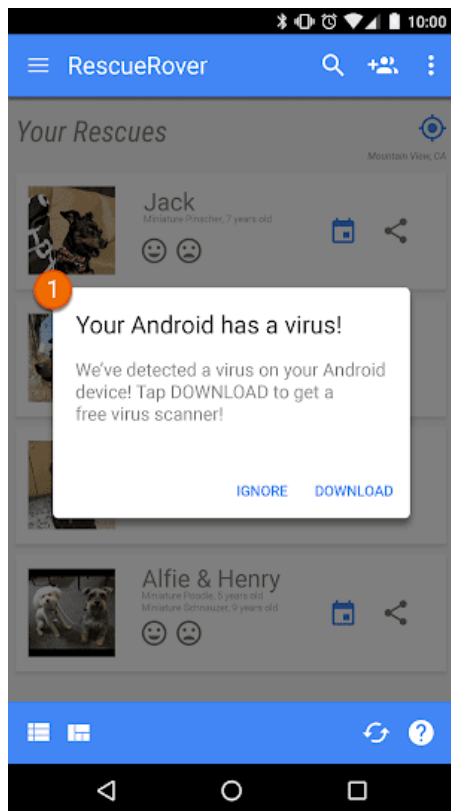
- En app, der gengiver annoncer, der ikke er synlige for brugeren.
- En app, der automatisk genererer klik på annoncer, uden at det er brugerens hensigt, eller som genererer tilsvarende netværkstrafik for svigagtigt at give klikkredit.
- En app, der sender falske installationsklik for at modtage betaling for installationer, der ikke stammer fra afsenderens netværk.
- En app, der viser pop op-annoncer, når brugeren ikke bruger appens brugerflade.
- Afgivelse af urigtige oplysninger om en apps annoncebeholdning, f.eks. en app, der kommunikerer til annoncenetværk, at den kører på en iOS-enhed, når den faktisk kører på en Android-enhed, eller en app, der giver urigtige oplysninger om det pakkenavn, der tjenes penge på.

Uautoriseret brug eller efterligning af systemfunktioner

Vi tillader ikke apps eller annoncer, der efterligner eller forstyrrer systemfunktioner som f.eks. underretninger eller advarsler. Notifikationer på systemniveau må kun bruges i en apps integrerede funktioner, f.eks. en app fra et flyselskab, der underretter brugerne om særtilbud, eller et spil, der underretter brugerne om kampagner i spillet.

Her er nogle eksempler på typiske overtrædelser:

- Apps eller annoncer, der vises via en systemnotifikation eller -underretning:



① Den systemnotifikation, der vises i denne app, bruges til at levere en annonce.

Du kan se flere eksempler med annoncer i [annoncepolitikken](#).

Efterligning

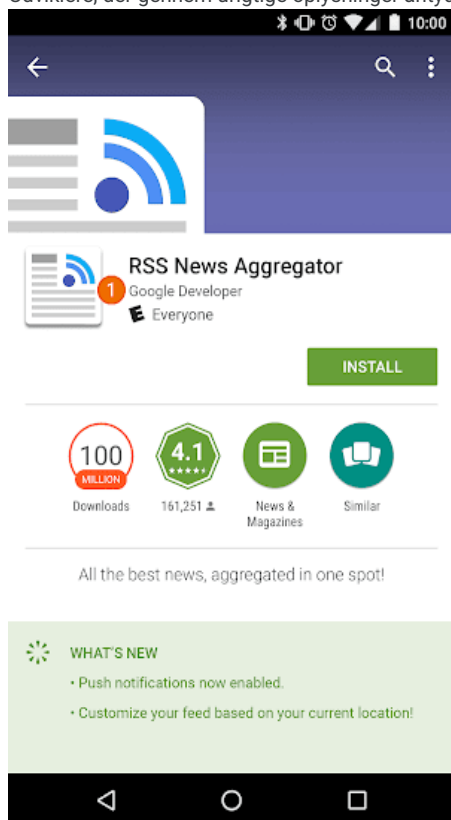
Når udviklere efterligner andre udviklere eller deres apps, vildleder det brugerne og skader udviklerfællesskabet. Vi forbyder apps, der vildleder brugerne ved at efterligne andre udviklere eller apps.

Efterligning

Vi tillader ikke apps, der vildleder brugerne ved at efterligne andre (f.eks. en anden udvikler, virksomhed eller enhed) eller en anden app. Antyd ikke, at din app er relateret til eller godkendt af nogen, hvis det ikke er tilfældet. Sørg for ikke at bruge appikoner, beskrivelser, titler eller elementer i apps, der kan vildlede brugerne om din apps forhold til andre personer eller en anden app.

Her er nogle eksempler på typiske overtrædelser:

- Udviklere, der gennem urigtige oplysninger antyder et forhold til en anden virksomhed/udvikler:



① Det udgivernavn, der er angivet for denne app, antyder en officiel relation til Google, selv om en sådan relation ikke findes.

- Appnavne og -ikoner, der ligner eksisterende produkter eller tjenester så meget, at brugerne kan blive vildledt:



Indtægtsgenerering og annoncer

Google Play understøtter en række forskellige strategier til indtægtsgenerering for udviklere og brugere, f.eks. distributionsplaner, produkter i apps, abonnementer og annoncebaserede modeller. For at sikre den bedst mulige brugeroplevelse kræver vi, at du overholder disse politikker.

Betalinger

Apps, der anvender køb i butikken eller i appen, skal overholde følgende retningslinjer:

Køb i butikken: Udviklere, der opkræver betaling for apps og downloads i Google Play, skal bruge Google Plays betalingssystem.

Køb i appen:

- Udviklere, der tilbyder produkter i et spil, der downloades i Google Play, eller giver adgang til spilindhold, skal bruge [Google Play Fakturering i appen](#) som betalingsmetode.
- Udviklere, der tilbyder produkter i en anden appkategori, som downloades i Google Play, skal bruge [Google Play Fakturering i appen](#) som betalingsmetode, medmindre:
 - Betalingen udelukkende er for fysiske varer
 - Betalingen er for digitalt indhold, som kan bruges uden for selve appen (f.eks. sange, der kan afspilles på andre musikafspillere).
- Virtuelle valutaer i apps må kun anvendes i den app eller i det spil, som de er blevet købt til.
- Udviklerne må ikke vildlede brugerne i forhold til de apps, de sælger, eller i forhold til tjenester, varer, indhold eller funktionalitet i de apps, de sælger. Hvis din produktbeskrivelse i Google Play henviser til funktioner i appen, som kræver et særskilt gebyr eller tillægsgebyr, skal din beskrivelse tydeligt oplyse brugerne om, at adgang til disse funktioner kræver betaling.
- Apps, der tilbyder mekanismer til at modtage vilkårlige virtuelle genstande fra et køb (f.eks. "lootboxes"), skal tydeligt angive sandsynligheden for at modtage disse genstande forud for købet.

Her er nogle eksempler på produkter, der understøttes af Google Play Fakturering i appen:

- **Virtuelle spilprodukter**, bl.a. mønter, ædelstene, ekstra liv eller ture, særlige ting eller udstyr, figurer eller avatarer, yderligere niveauer eller spilletid.
- **Appfunktionalitet eller -indhold** som f.eks. en reklamefri version af en app eller nye funktioner, som ikke er tilgængelige i den gratis version.
- **Abonnementstjenester** som f.eks. digitale publikationer, også når de leveres sammen med fysiske udgaver, samt sociale netværkstjenester og streaming af musik, videoer, bøger eller andre medietjenester.
- **Softwareprodukter i skyen**, bl.a. tjenester til lagring af data, produktivtetssoftware til virksomheder og software til økonomistyring.

Her er nogle eksempler på produkter, der på nuværende tidspunkt ikke understøttes af Google Play Fakturering i appen:

- **Detailvarer** som f.eks. dagligvarer, tøj, husholdningsartikler og elektronik.
- **Servicegebyrer**, herunder taxa- og transporttjenester, rengøringstjenester, madlevering, flybilletter og billetter til arrangementer.
- **Engangsgebyrer eller faste gebyrer for medlemskab**, herunder medlemskab til et fitnesscenter, loyalitetsprogrammer eller klubber, der tilbyder tilbehør, tøj eller andre fysiske produkter.
- **Engangsbetalinger**, herunder P2P-betalinger (peer-to-peer), online auktioner og donationer.
- **Elektronisk betaling af fakturaer**, herunder betalingskortfakturaer, forsyning og kabel- eller teletjenester

Bemærk! Vi tilbyder Google Pay API til apps, hvor der sælges fysiske produkter og serviceydelser. Du kan få flere oplysninger ved at gå til vores [udviklerside for Google Pay](#).

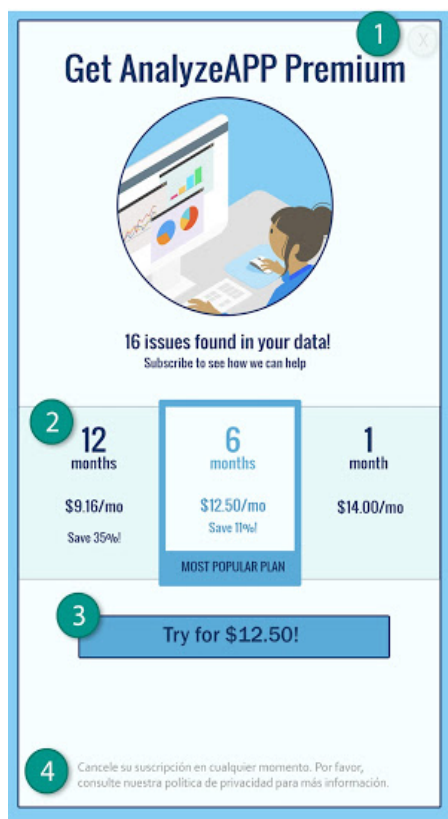
Abonnementer

Som udvikler må du ikke vildlede brugerne om de abonnementstjenester eller det abonnementsindhold, du tilbyder i din app. Det er meget vigtigt, at du tydeligt kommunikerer, hvad du tilbyder, i eventuelle kampagner i apps eller på splash-skærme.

I din app: Det skal være klart, hvad dit tilbud omfatter. Det vil sige, at du tydeligt skal angive vilkårene for tilbuddet, prisen på abonnementet, frekvensen for din faktureringscyklus, og om der kræves abonnement for at bruge appen. Det bør ikke være nødvendigt for brugerne at foretage sig yderligere for at se oplysningerne.

Her er nogle eksempler på typiske overtrædelser:

- Månedssabonnementer, hvor brugerne ikke oplyses om, at abonnementerne automatisk fornyes hver måned, og at brugerne debiteres hver måned.
- Årsabonnementer, hvor den månedlige pris fremhæves.
- Abonnementspriser og -vilkår, som ikke er fuldstændigt tilpasset til det lokale marked.
- Kampagner i apps, hvor det ikke tydeligt fremgår, at en bruger har adgang til indhold uden et abonnement (hvis det er relevant).
- Navne på varenumre, som ikke nøjagtigt afspejler typen af abonnement, f.eks. "Gratis prøveperiode" ved et abonnement med automatisk debitering.



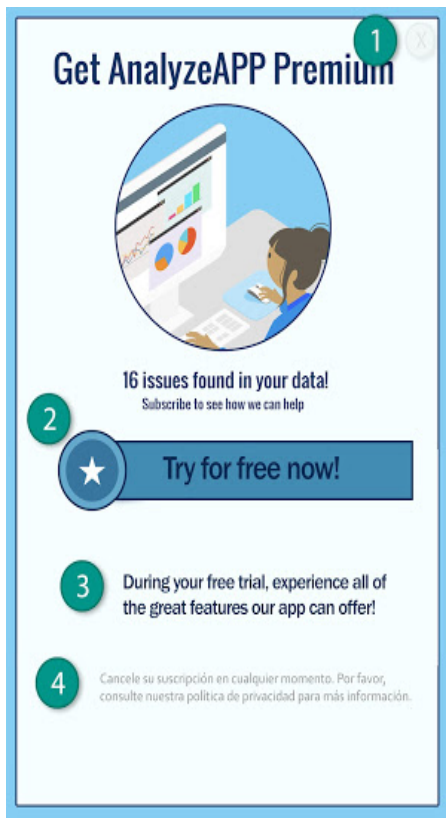
- Knappen til afvisning vises ikke tydeligt nok, så brugerne forstår muligvis ikke, at de kan få adgang til funktionerne uden at benytte sig af tilbuddet om abonnement.
- Priserne vises kun på månedsbasis i tilbuddet, så brugerne forstår muligvis ikke, at de bliver debiteret for seks måneder, når de opretter abonnementet.
- Det er kun introduktionsprisen, der vises i tilbuddet, så brugerne forstår muligvis ikke, at de automatisk bliver debiteret, når introduktionsperioden udløber.
- Tilbuddet skal oversættes til samme sprog som vilkårene og betingelserne, så brugerne forstår tilbuddets fulde omfang.

Gratis prøveperioder og velkomstilbud

Inden en bruger opretter abonnement: Du skal klart og præcist beskrive vilkårene for dit tilbud, inklusive varighed, pris og en beskrivelse af det indhold eller de tjenester, der er tilgængelige. Sørg for at give dine brugere besked om, hvordan og hvornår en gratis prøveperiode ændres til et betalingsabonnement, hvor meget betalingsabonnementet koster, og at brugeren kan opsige, hvis vedkommende ikke vil overgå til et betalt abonnement.

Her er nogle eksempler på typiske overtrædelser:

- Tilbud, hvor det ikke tydeligt er forklaret, hvor længe den gratis prøveperiode eller introduktionsprisen er gældende.
- Tilbud, hvor det ikke tydeligt er forklaret, at brugeren automatisk tilmeldes et betalingsabonnement, når tilbudsperioden udløber.
- Tilbud, hvor det ikke tydeligt fremgår, at en bruger kan få adgang til indholdet uden en prøveperiode (hvis det er relevant).
- Priser og vilkår for tilbuddet, som ikke er fuldstændigt tilpasset til det lokale marked.



- ① Knappen til afvisning vises ikke tydeligt nok, så brugerne forstår muligvis ikke, at de kan få adgang til funktionerne uden at tilmelde sig den gratis prøveperiode.
- ② Tilbuddet fremhæver den gratis prøveperiode, så brugerne forstår muligvis ikke, at de automatisk bliver debiteret efter prøveperiodens udløb.
- ③ Tilbuddet angiver ikke en specifik prøveperiode, så brugerne forstår muligvis ikke, hvor længe de har gratis adgang til abonnementsindholdet.
- ④ Tilbuddet skal oversættes til samme sprog som vilkårene og betingelserne, så brugerne forstår tilbuddets fulde omfang.

Administration og opsigelse af abonnementer

Som udvikler skal du sørge for, at din app tydeligt oplyser brugeren om, hvordan vedkommende kan administrere eller opsiges sit abonnement.

Det er dit ansvar at informere dine brugere om eventuelle ændringer i dine abonnementer og politikker for opsigelse og refundering samt at sikre, at politikkerne er i overensstemmelse med gældende lovgivning.

Annoncer

Vi tillader ikke apps, der indeholder vildledende eller forstyrrende annoncer. Annoncer må kun vises i den app, der leverer dem. Vi betragter de annoncer, der vises i din app, som en del af appen. De annoncer, der vises i din app, skal overholde alle vores politikker. Du kan få flere oplysninger om politikker for hasardspilannoncer ved at klikke [her](#).

Brug af placeringsdata til annoncer

Apps, der udvider brugen af tilladelsesbaserede data om enhedsplacering til annoncevisning, er underlagt politikken om [personlige og følsomme oplysninger](#) og skal også overholde følgende krav:

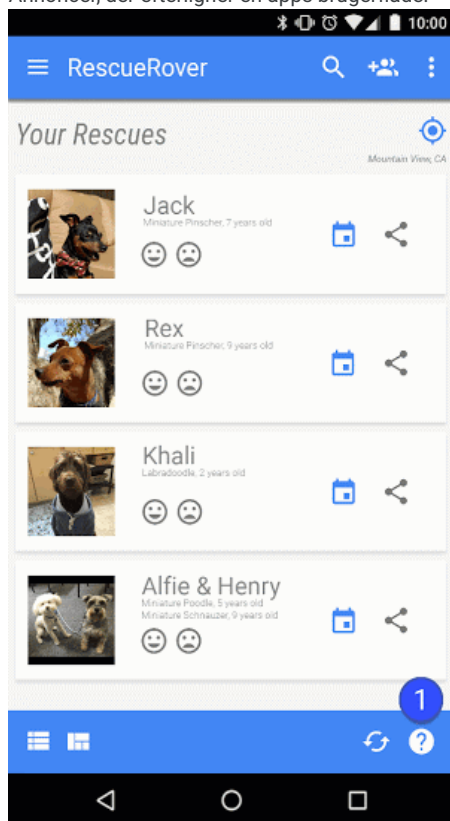
- Brug eller indsamling af tilladelsesbaserede data om enhedsplacering med henblik på annoncering skal være tydelig for brugeren og dokumenteret i appens obligatoriske privatlivspolitik samt indeholde links til relevante privatlivspolitikker for annoncenetværk, der omhandler brug af placeringsdata.
- I overensstemmelse med kravene om [adgangstilladelser til placering](#) må der kun anmodes om adgangstilladelser til placering for at implementere eksisterende funktioner eller tjenester i din app, og der må ikke anmodes om adgangstilladelser til enhedens placering udelukkende med henblik på brug af annoncer.

Vildledende annoncer

Annoncer må ikke simulere eller efterligne brugerfladen for apps, underretninger eller advarsler fra et operativsystem. Det skal være klart for brugeren, hvilken app der viser de enkelte annoncer.

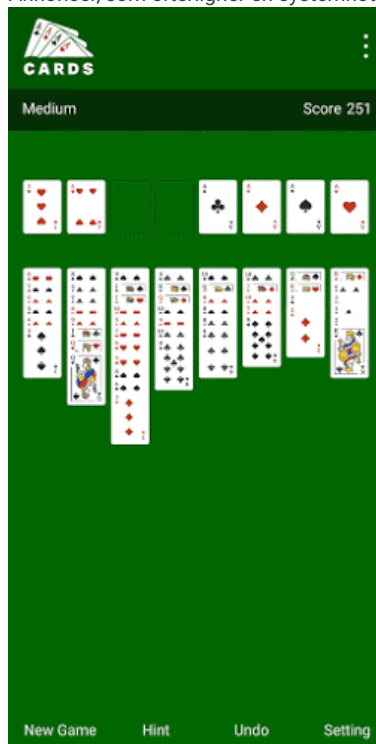
Her er nogle eksempler på typiske overtrædelser:

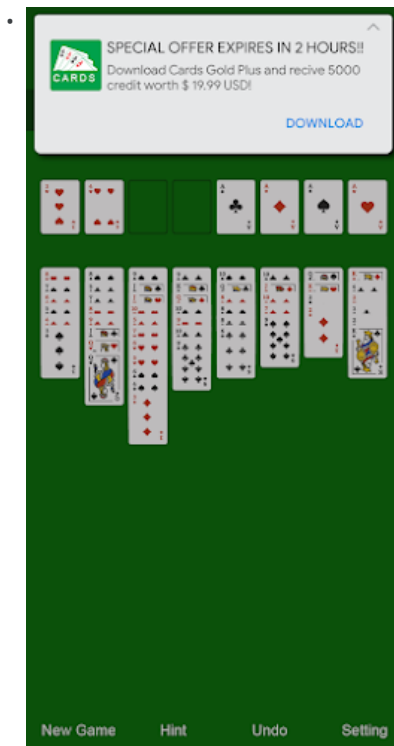
- Annoncer, der efterligner en apps brugerflade:



① Spørgsmålstegnet i denne app er en annonce, der omdirigerer brugeren til en ekstern landingsside.

- Annoncer, som efterligner en systemnotifikation:





Eksemplerne ovenfor viser annoncer, der efterligner forskellige systemnotifikationer.

Indtægtsgenerering via låseskærmen

Medmindre låseskærmen er det eksklusive formål med en app, må apps ikke præsentere annoncer eller funktioner, der genererer indtægter via den låste skærm på en enhed.

Forstyrrende annoncer

Forstyrrende annoncer er annoncer, der vises til brugerne på uventede måder, der kan resultere i utilsigtede klik eller forringer eller forstyrrer brugbarheden af enhedens funktioner.

Din app må ikke tvinge en bruger til at klikke på en annonce eller indsende personlige oplysninger til annonceringsformål, før brugeren kan bruge appen fuldt ud. Mellemliggende annoncer må kun vises inde i den app, der leverer dem. Hvis din app viser mellemliggende annoncer eller andre annoncer, der forstyrrer normal brug, skal de nemt kunne afvises uden konsekvenser.

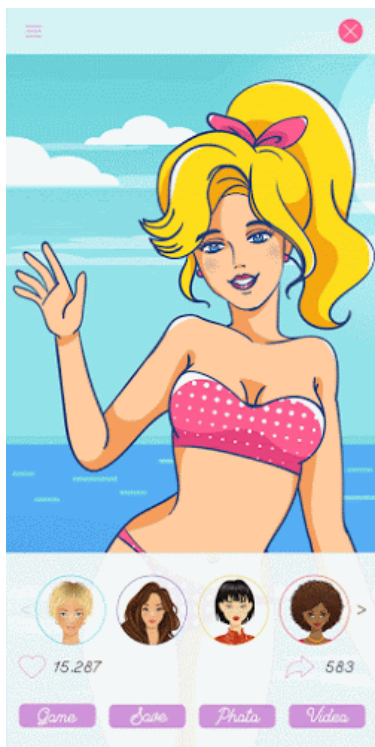
Her er nogle eksempler på typiske overtrædelser:

- Annoncer, der fylder hele skærmen eller forstyrrer normal brug, og som ikke tydeligt angiver, hvordan annoncen kan afvises:

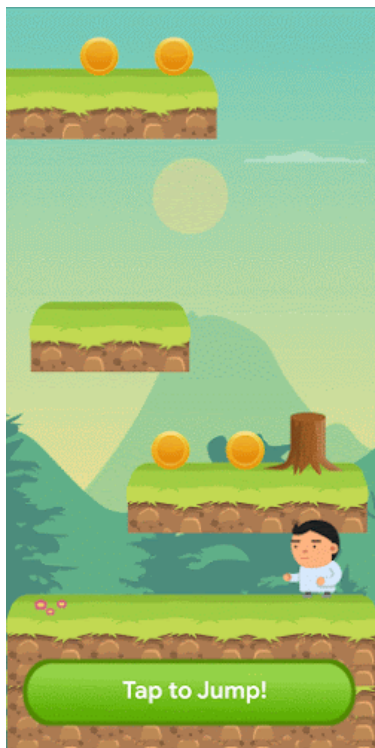


① Denne annonce har ikke en afvisningsknap.

- Annoncer, der tvinger brugeren til at klikke videre fra annoncen ved hjælp af en falsk afvisningsknap eller ved at få annoncer til pludselig at dukke op i områder af appen, uanset om brugeren normalt trykker på en anden funktion.



En annonce, der bruger en falsk afvisningsknap



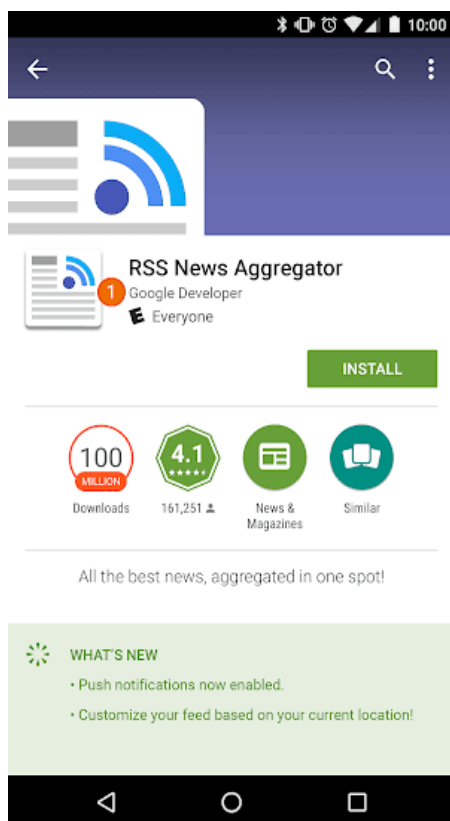
En annonce, der pludselig vises i et område, hvor brugeren er vant til at trykke for at bruge funktioner i appen

Forstyrrelse af apps, tredjepartsannoncer eller enhedens funktionalitet

Annoncer, der er knyttet til din app, må ikke forstyrre andre apps, annoncer eller enhedens drift, herunder system- eller enhedsknapper og porte. Dette omfatter overlejring, ledsagende funktionalitet eller annonceenheder i widgets. Annoncer må kun vises i den app, der leverer dem.

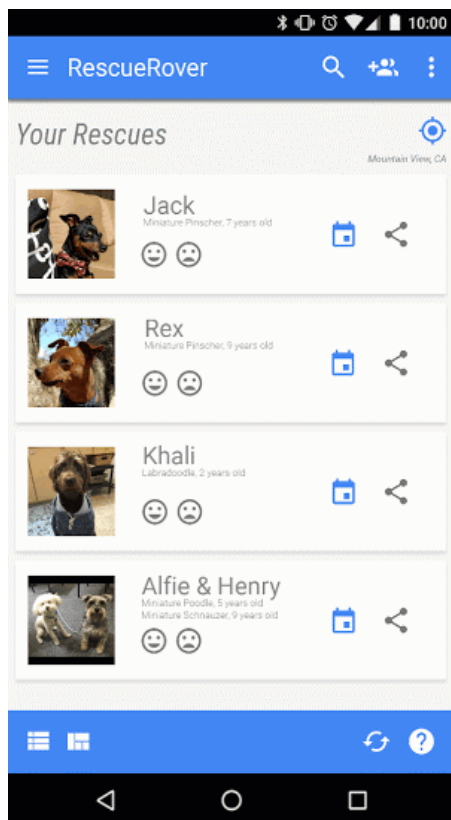
Her er nogle eksempler på typiske overtrædelser:

- Annoncer, der vises uden for den app, der leverer dem:



Beskrivelse: Brugeren navigerer til startskærmen fra denne app og pludselig vises der en annonce på startskærmen.

- Annoncer, der udløses af knappen Start eller andre funktioner, som udelukkende er designet til at lukke appen:

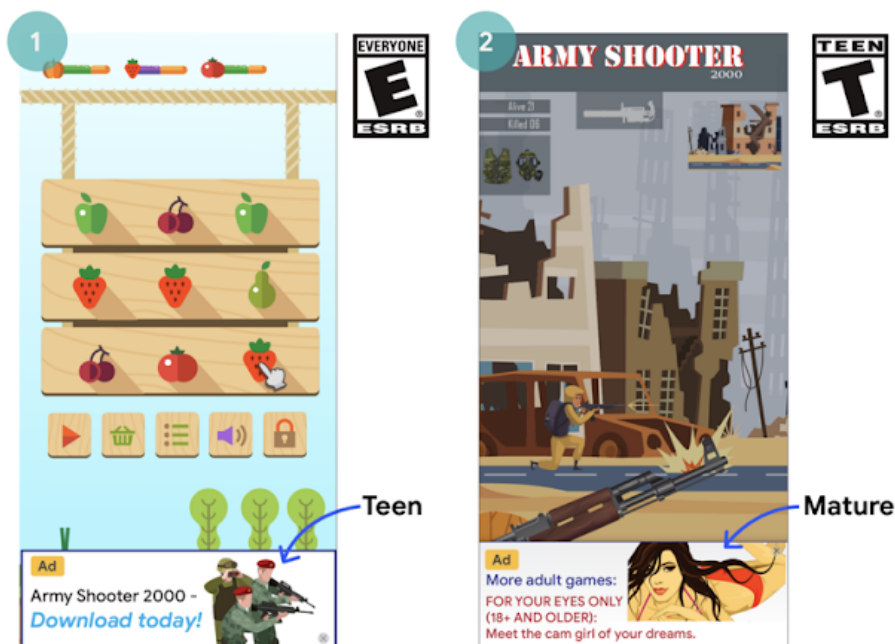


Beskrivelse: Brugeren forsøger at lukke appen og navigere til startskærmen, men i stedet forstyrres forløbet af en annonce.

Upassende annoncer

De annoncer, der vises i din app, skal være egnet til din apps tiltænkte målgruppe, også selvom indholdet i sig selv i øvrigt overholder vores politikker.

Her er et eksempel på en typisk overtrædelse:



- ① Denne annonce er upassende (teenagerindhold) for appens tiltænkte målgruppe (7+)
- ② Denne annonce er upassende (voksenindhold) for appens tiltænkte målgruppe (12+)

Brug af Androids annoncerings-id

Google Play-tjenester version 4.0 introducerede nye API'er og et id til brug for annonce- og analyseudbydere. Vilkårene for brugen af dette id er angivet nedenfor.

- **Brug:** Androids annoncerings-id må kun bruges til annoncering og brugeranalyser. Status for indstillingen "Fravælg interessebaseret annoncering" eller "Fravælg annoncetilpasning" skal bekræftes, hver gang id'et forsøger at få adgang.
- **Tilknytning til personhenførbare oplysninger eller andre id'er**
 - Annonceringsbrug: Annoncerings-id'et må ikke knyttes til vedvarende enheds-id'er (f.eks. SSAID, MAC-adresse eller IMEI) til nogen form for annonceringsformål. Annoncerings-id'et må kun knyttes til personhenførbare oplysninger med brugerens udtrykkelige samtykke.
 - Analysebrug: Annoncerings-id'et må kun knyttes til personhenførbare oplysninger eller vedvarende enheds-id'er (f.eks. SSAID, MAC-adresse eller IMEI) med brugerens udtrykkelige samtykke.
- **Respekter brugernes valg.** I forbindelse med nulstilling må et nyt annoncerings-id ikke knyttes til et tidligere annoncerings-id eller data, der stammer fra et tidligere annoncerings-id, uden brugerens udtrykkelige samtykke. Desuden skal du respektere brugerens indstilling for "Fravælg interessebaseret annoncering" eller "Fravælg annoncetilpasning". Hvis en bruger har aktiveret denne indstilling, må du ikke bruge annoncerings-id'et til at oprette brugerprofiler til annonceringsformål eller til at målrette tilpassede annoncer mod brugere. De tilladte aktiviteter omfatter kontekstmålretning, frekvensbegrænsning, konverteringssporing, rapportering og sikkerhed samt registrering af svindel.
- **Gennemsigtighed for brugerne.** Registrering og brug af annoncerings-id'et og forpligtelserne i henhold til disse vilkår skal offentliggøres for brugerne i en juridisk fyldestgørende erklæring om privatliv. Du kan få flere oplysninger om vores standarder for beskyttelse af personlige oplysninger ved at læse vores politik om [brugerdata](#).
- **Overholdelse af servicevilkårene.** Annonce-id'et må kun anvendes i overensstemmelse med disse vilkår. Dette gælder også for alle de parter, som du deler det med som led i den daglige drift. Alle apps, der uploades til eller udgives i Google Play, skal anvende annonce-id'et (når det er tilgængeligt på en enhed) i stedet for andre enheds-id'er til alle annoncerrelaterede formål.

Program for annoncer til børn

Hvis du viser annoncer i din app, og målgruppen for din app kun omfatter børn som beskrevet i [familiepolitikken](#), skal du bruge annonce-SDK'er, som ved selvklassificering har bekræftet, at de overholder Google Plays politikker, herunder kravene til certificering af annonce-SDK'er nedenfor. Hvis målgruppen for din app omfatter både børn og ældre brugere, skal du implementere metoder til aldersbekræftelse og sørge for, at de annoncer, der vises til børn, udelukkende stammer fra en af disse selvcertificerede annonce-SDK'er. Det er et krav, at apps i programmet For hele familien kun bruger selvcertificerede annonce-SDK'er.

Brug af Google Plays certificerede annonce-SDK'er er kun påkrævet, hvis du bruger annonce-SDK'er til at vise annoncer til børn. Følgende er tilladt uden selvcertificering af en annonce-SDK hos Google Play, men du er stadig ansvarlig for at sikre,

at dit annonceindhold og dine metoder til indsamling af data overholder Plays [brugerdatapolitik](#) og [familiepolitik](#):

- Egneannoncering, hvor du bruger SDK'er til at administrere krydspromovering af dine apps eller andre medier eller merchandising, som du selv ejer
- Indgåelse af direkte aftaler med annoncører, hvor du bruger SDK'er til administration af beholdning

Krav til certificering af annonce-SDK'er

- Definer problematisk annonceindhold og -adfærd, og forbyd det i annonce-SDK'ens vilkår eller politikker. Definitionerne skal overholde Plays programpolitikker for udviklere.
- Opret en metode til klassificering af dit annoncemateriale i henhold til aldersgrupper. Aldersgrupperne skal som minimum omfatte grupperne Alle og Voksne. Klassificeringsmetoden skal stemme overens med den metode, som Google stiller til rådighed for SDK'er, når de har udfyldt interesseformularen nedenfor.
- Tillad, at udgivere anmoder om børneorienteret behandling med henblik på annoncevisning pr. anmodning eller pr. app. Denne behandling skal overholde gældende love og bestemmelser som f.eks. den amerikanske [Children's Online Privacy and Protection Act \(COPPA\)](#) og [EU's persondataforordning \(GDPR\)](#). Google Play kræver, at annonce-SDK'er deaktiverer tilpassede annoncer, interessebaseret annoncering og remarketing som en del af den børneorienterede behandling.
- Giv udgivere mulighed for at vælge annonceformater, der overholder [Plays politik om familieannoncer og indtægtsgenerering](#), og opfylde kravene i [programmet Lærergodkendte apps](#).
- Sørg for, at annoncematerialet er blevet gennemgået, og at privatlivsindikatorerne formidles til byderne, når budgivning i realtid anvendes til at vise annoncer til børn.
- Giv Google tilstrækkelige oplysninger, f.eks. de oplysninger, der angives i [interesseformularen](#) nedenfor, til at bekræfte annonce-SDK'ens overholdelse af alle certificeringskrav, og reager rettidigt på eventuelle efterfølgende anmodninger om oplysninger.

Bemærk! Annonce-SDK'er skal understøtte annoncevisning, som overholder alle relevante vedtægter og bestemmelser vedrørende børn, der måtte gælde for deres udgivere.

Formidlingskrav til visningsplatforme, når der vises annoncer til børn:

- Brug kun Play-certificerede annonce-SDK'er, eller implementer sikkerhedsforanstaltninger, der er nødvendige for at sikre, at alle annoncer, der vises via formidling, opfylder disse krav
- Videregiv de oplysninger, der er nødvendige for, at formidlingsplatforme kan angive klassificeringen af annonceindholdet og enhver relevant børneorienteret behandling.

Udviklerne kan se en [liste over selvcertificerede annonce-SDK'er](#) her.

Udviklerne kan også dele denne [interesseformular](#) med annonce-SDK'er, der gerne vil selvcertificeres.

Profilside i Play Butik og promovering

Promoveringen og synligheden af din app har stor indflydelse på kvaliteten i appbutikken. Undgå profilsider i Play Butik, der indeholder spam, promovering af lav kvalitet og forsøg på kunstigt at forbedre appens synlighed i Google Play.

Promovering af apps

Vi tillader ikke apps, som direkte eller indirekte anvender eller drager nytte af promoveringer, der er vildledende eller skadelige over for brugere eller fællesskabet af udviklere. Dette omfatter apps, der benytter sig af følgende adfærd:

- Brug af vildledende annoncer på websites, i apps eller andre ejendomme, herunder underretninger, der ligner systemunderretninger og -advarsler.
- Promoverings- eller installationsstrategier, der omdirigerer brugerne til Google Play eller til at downloade apps, uden at brugeren selv vælger det.
- Uopfordret promovering via sms-tjenester.

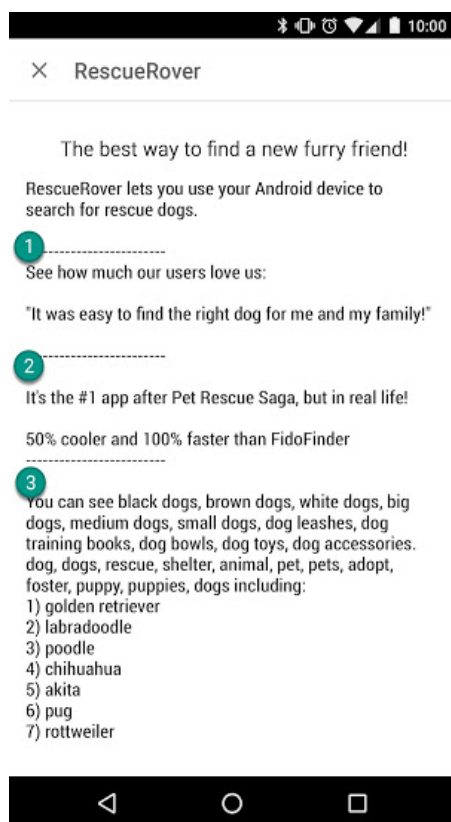
Det er dit ansvar at sikre, at alle netværk eller associerede virksomheder, der er tilknyttet din app, overholder disse politikker, og at de ikke benytter forbudte promoveringsmetoder.

Metadata

Vi tillader ikke apps, der er forkert formateret, eller som har ikke-beskrivende, irrelevante, upassende eller en overdreven mængde metadata, herunder, men ikke begrænset til, appens beskrivelse, udviklernavn, titel, ikon, screenshots og promoveringsbilleder. Udviklere skal angive en tydelig og velskrevet beskrivelse af deres app. Vi tillader ikke udtalelser uden kilde eller udtalelser fra anonyme brugere i appbeskrivelsen.

Ud over de krav, der angives her, kan specifikke Play-udviklerpolitikker kræve, at du angiver yderligere metadataoplysninger.

Her er nogle eksempler på typiske overtrædelser:



- ① Udtalelser, der ikke er tilskrevet nogen, eller udtalelser fra anonyme brugere
- ② Sammenligning af data for apps eller brands
- ③ Blokke af ord eller lodrette/vandrette ordlister

Her er nogle eksempler på upassende tekst, billeder eller videoer på din profilside:

- Billeder eller videoer med seksuelt orienteret indhold. Undgå seksuelt orienterede billeder, der viser bryster, balder, kønsdele, andre feticherede kropsdele eller andet feticheret indhold, uanset om der er tale om illustrerede eller virkelige gengivelser.
- Brug af groft, vulgært eller andet sprog, der er upassende for en generel målgruppe på din apps profilside i Google Play.
- Fremtrædende afbildning af udpenslet vold i appikoner, billeder til promovring eller videoer.
- Skildringer af ulovlig brug af medicin eller narkotika. Selv undervisningsrettet, dokumentarisk, videnskabeligt eller kunstnerisk indhold skal være egnet til alle målgrupper på profilsiden i Play Butik.

Her er et par af de bedste fremgangsmåder:

- Fremhæv fordelene ved din app. Del interessante og spændende fakta om din app med brugerne for at gøre dem opmærksomme på, hvad der gør din app unik.
- Sørg for, at din apps navn og beskrivelse beskriver appens funktionalitet korrekt.
- Undgå at gentage søgeord eller bruge irrelevante søgeord eller referencer.
- Sørg for, at din appbeskrivelse er kortfattet og præcis. Kortere beskrivelser giver ofte en bedre brugeroplevelse, især på enheder med mindre skærme. En overdreven tekstmængde, forkert formatering og for mange detaljer eller gentagelser kan resultere i, at denne politik overtrædes.
- Husk, at din profilside skal være egnet for alle. Undgå at bruge upassende tekst, billeder eller videoer på din profilside, og følg ovenstående retningslinjer.

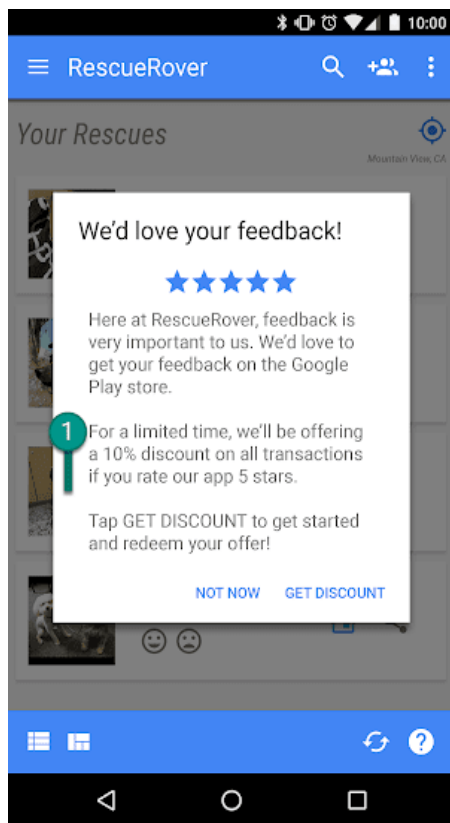
Brugerbedømmelser, anmeldelser og installationer

Udviklere må ikke forsøge at manipulere placeringen af apps i Google Play. Dette omfatter, men er ikke begrænset til, forsøg på at forbedre produktets bedømmelser, anmeldelser eller antal installationer ved brug af ulovlige metoder, f.eks.

falske eller incitamentdrevne installationer, anmeldelser og bedømmelser.

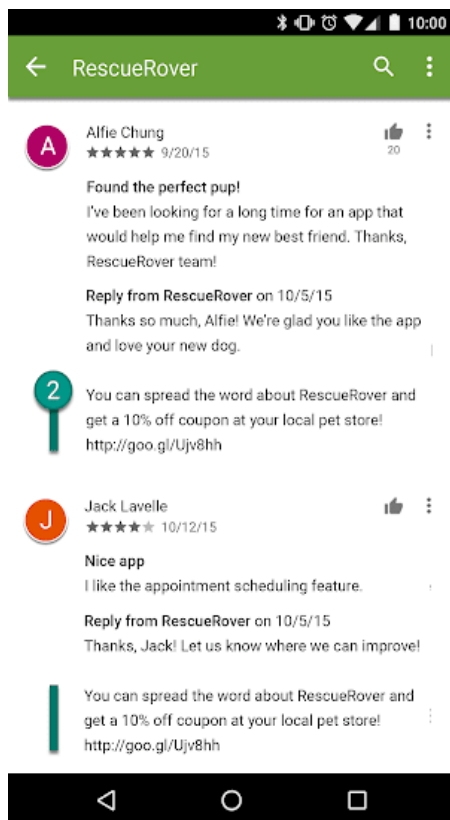
Her er nogle eksempler på typiske overtrædelser:

- Opfordring til brugerne om at bedømme din app samtidig med, at du giver brugerne et incitament:



① Denne notifikation tilbyder brugerne en rabat som tak for en god bedømmelse.

- Gentagne indsendelser af bedømmelser for at påvirke appens placering i Google Play.
- Indsendelse eller opfordring til at indsende anmeldelser med upassende indhold, f.eks. oplysninger om associerede virksomheder, kuponer, spilkoder, mailadresser eller links til websites eller andre apps:



② Denne anmeldelse opfordrer brugerne til at promovere appen RescueRover ved at tilbyde en kupon.

Bedømmelser og anmeldelser er udtryk for appkvalitet. Brugerne skal kunne stole på, at de er autentiske og relevante. Her kan du se, hvordan du bedst besvarer brugeranmeldelser:

- Sørg for, at dit svar fokuserer på de faktiske spørgsmål i brugerens kommentarer, og undlad at bede om en højere bedømmelse.
- Medtag henvisninger til nyttige ressourcer som f.eks. en supportadresse eller en side med ofte stillede spørgsmål.

Indholdsklassificeringer

Indholdsklassificeringer i Google Play leveres af IARC (International Age Rating Coalition) og er designet til at hjælpe udviklere med at formidle lokalt relevante indholdsklassificeringer til brugerne. Regionale IARC-myndigheder håndhæver retningslinjer, som anvendes til at afgøre modenhedsniveauet for indholdet i en app. Vi tillader ikke apps uden indholdsklassificering i Google Play.

Sådan bruges indholdsklassificeringer

Indholdsklassificeringerne bruges til at oplyse forbrugerne, især forældre, om potentielt anstødeligt indhold i en app. De hjælper også med at filtrere eller blokere dit indhold i bestemte geografiske områder eller for bestemte brugere, hvor dette er lovkrav, og med at vurdere, om din app er egnet til særlige programmer for udviklere.

Sådan tildes indholdsklassificeringer

Du modtager en indholdsklassificering ved at udfylde et [spørgeskema til klassificering i Play Console](#), der indeholder spørgsmål om karakteren af indholdet i dine apps. Din app tildes en indholdsklassificering af flere klassificeringsmyndigheder ud fra dine svar i spørgeskemaet. En vildledende beskrivelse af appens indhold kan resultere i fjernelse eller suspendering, så det er vigtigt at give nøjagtige svar i spørgeskemaet til indholdsklassificering.

Du kan forhindre, at din app angives som "Ikke klassificeret", ved at udfylde spørgeskemaet til indholdsklassificering for hver ny app, du indsender til Play Console, og for alle eksisterende apps, der er aktive i Google Play.

Hvis du foretager ændringer i appens indhold eller funktioner, som kan påvirke svarene i spørgeskemaet til klassificering, skal du indsende et nyt spørgeskema i Play Console.

Du kan få flere oplysninger om de forskellige [klassificeringsmyndigheder](#), og om hvordan du udfylder spørgeskemaet til indholdsklassificering, ved at gå til [Hjælp](#).

Appel af klassificeringer

Hvis du ikke er enig i den klassificering, der er tildelt din app, kan du appellere direkte til IARC-klassificeringsmyndigheden via det angivne link i mailen med dit klassificeringscertifikat.

Nyheder

En app, der beskriver sig selv som en "nyhedsapp" i Google Play, skal overholde alle følgende krav.

Nyhedsapps, der kræver, at en bruger køber et medlemskab, skal give brugerne en forhåndsvisning af indholdet, før de foretager et køb.

Nyhedsapps SKAL:

- Oplyse ejerskabsinfo om nyhedsudgiveren og dennes bidragydere, herunder, men ikke begrænset til, det officielle website for de nyheder, der udgives i din app, gyldige kontaktoplysninger, der kan bekræftes, og den oprindelige udgiver af hver artikel
- Have et website eller en side i appen med gyldige kontaktoplysninger til nyhedsudgiveren.

Nyhedsapps MÅ IKKE:

- Indeholde væsentlige stave- og grammatikfejl
- Kun indeholde statisk indhold (f.eks. indhold, der er flere måneder gammelt)
- Have affiliate markedsføring eller annonceomsætning som deres primære formål.

Nyhedsapps, der samler indhold fra forskellige udgivelseskilder, skal tydeligt angive udgivelseskilden for indholdet i appen, og hver af kilderne skal opfylde kravene i politikken vedrørende nyheder.

Spam og minimumfunktionalitet

Apps skal som minimum give brugerne en grundlæggende funktionalitet og en hæderlig brugeroplevelse. Apps, som går ned, på anden vis ikke leverer en funktionel brugeroplevelse, eller som udelukkende har til formål at spamme brugerne eller Google Play, er ikke apps, som tilføjer noget meningsfuldt til kataloget.

Spam

Vi tillader ikke apps, der spammer brugerne eller Google Play, f.eks. apps, der sender brugerne uopfordrede meddelelser, kopiapps eller apps af lav kvalitet.

Meddelelssespam

Vi tillader ikke apps, der sender sms-beskeder, e-mails eller andre meddelelser på vegne af brugeren uden at give brugeren mulighed for at bekræfte indholdet og de tilsigtede modtagere.

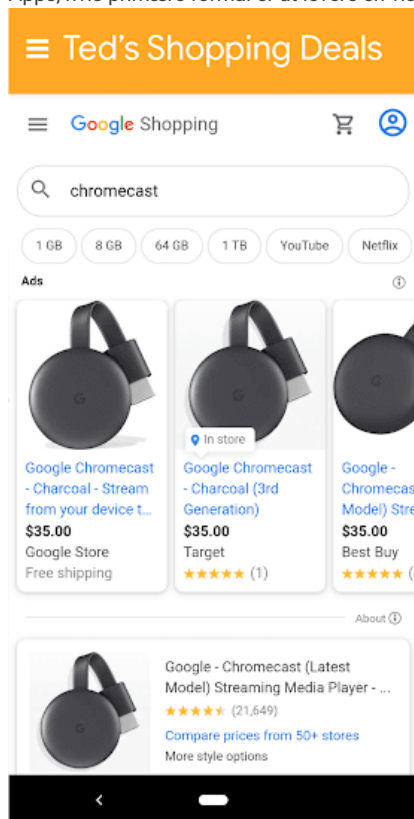
Webvisninger og associeret spam

Vi tillader ikke apps, hvis primære formål det er at generere associeret trafik til et website eller levere en visning af et website uden tilladelse fra websiteejeren eller -administratoren.

Her er nogle eksempler på typiske overtrædelser:

- En app, hvis primære formål det er at generere henvisningstrafik til et website for at opnå anerkendelse for brugertilmeldinger eller køb på det pågældende website.

- Apps, hvis primære formål er at levere en visning af et website uden tilladelse:



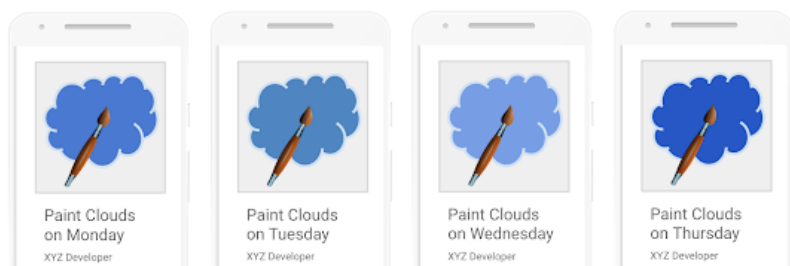
Denne app kaldes "Ted's Shopping Deals" og leverer ganske enkelt en webvisning af Google Shopping.

Gentaget indhold

Vi tillader ikke apps, der bare giver brugerne den samme oplevelse som andre apps, der allerede findes i Google Play. Apps bør tilføje værdi for brugerne gennem unikt indhold og unikke tjenester.

Her er nogle eksempler på typiske overtrædelser:

- Kopiering af indhold fra andre apps, uden at der tilføjes originalt indhold eller værdi.
- Oprettelse af flere apps, hvor funktionerne, indholdet og brugeroplevelsen er meget ens. Hvis hver af disse apps kun har lidt indhold, bør udviklerne overveje at lave én app, hvor alt indholdet er samlet.



Lavet til annoncer

Vi tillader ikke apps, hvis primære formål er at vise annoncer.

Her er nogle eksempler på typiske overtrædelser:

- Apps, hvor der er mellemliggende annoncer efter hver brugerhandling, herunder, men ikke begrænset til, klik, strøg osv.

Minimumfunktionalitet

Sørg for, at din app giver en stabil og engagerende brugeroplevelse med gode svartider.

Her er nogle eksempler på typiske overtrædelser:

- Apps, der er udviklet uden at have et formål eller en funktion

Apps, der ikke virker

Vi tillader ikke apps, som går ned, gennemtvinger lukning, fryser eller på anden måde fungerer unormalt.

Her er nogle eksempler på typiske overtrædelser:

- Apps, der **ikke kan installeres**
- Apps, der kan installeres, men **ikke indlæses**
- Apps, der kan indlæses, men som **ikke svarer**

Andre programmer

Apps, der er designet til andre Android-oplevelser og distribueres via Google Play, skal overholde de øvrige indholdspolitikker i dette politikcenter og kan desuden også være underlagt programspecifikke politikkrav. Sørg for gennemgå listen nedenfor for at afgøre, om nogen af politikkerne gælder for din app.

Android Instant Apps

Vores mål med Android Instant Apps er at skabe tiltalende, gnidningsløse brugeroplevelser og samtidig følge de højeste standarder for sikkerhed og privatliv. Vores politikker er udformet, så de understøtter dette mål.

Udviklere, der vælger at distribuere Android Instant Apps via Google Play, skal overholde følgende politikker, foruden alle andre [programpolitikker for udviklere i Google Play](#).

Identitet

I instant-apps med loginfunktion skal udviklerne integrere [Smart Lock til adgangskoder](#).

Understøttelse af links

Android Instant Apps-udviklere skal understøtte links til andre apps korrekt. Hvis udviklerens instant-apps eller installerede apps indeholder links, der eventuelt kan føre til en instant-app, skal udvikleren sende brugerne til den pågældende instant-app, og ikke f.eks. vise linkene i [Webvisning](#).

Tekniske specifikationer

Udviklere skal overholde Googles tekniske specifikationer og krav for Android Instant Apps, som til enhver tid kan ændres, herunder dem, der er angivet i [vores offentlige dokumenter](#).

Tilbud om appinstallation

Instant apps må tilbyde brugeren den installerbare app, men det må ikke være det primære formål med en instant app. Ved tilbud om installation skal udviklerne:

- Bruge [Material Design-ikonet "hent app"](#) og etiketten "installer" til installationsknappen.
- Der må ikke være mere end to eller tre implicitte installationsopfordringer i deres instant-app.
- Der må ikke bruges et banner eller andre annoncelignende teknikker til at vise brugerne en installationsopfordring.

Du kan få flere oplysninger om instant-apps og retningslinjerne for brugeroplevelsen ved at gå til siden med [optimale løsninger til brugeroplevelsen](#).

Ændringer af enhedstilstand

Instant apps må ikke foretage ændringer på brugerens enhed, der varer længere end instant app-sessionen. Instant apps må f.eks. ikke ændre brugerens baggrund eller oprette en widget på startskærmen.

Appsynlighed

Udviklere skal sikre, at instant apps er synlige for brugeren, så denne altid er klar over, at instant appen kører på vedkommendes enhed.

Enhedsidentifikatorer

Instant apps må ikke få adgang til enhedsidentifikatorer, der hverken (1) forsvinder, når instant appen holder op med at køre, eller (2) kan nulstilles af brugeren. Eksempler omfatter, men er ikke begrænset til:

- Buildets serienummer

- MAC-adresser på eventuelle netværkschips
- IMEI, IMSI

Instant apps må få adgang til telefonnummeret, hvis der opnås tilladelse på kørselstidspunktet. Udvikleren må ikke forsøge at identificere brugeren ved hjælp af disse identifikatorer eller på nogen anden måde.

Netværkstrafik

Netværkstrafik fra en instant-app skal være krypteret med en TLS-protokol såsom HTTPS.

Familier

Med Google Play får udviklere en solid platform til at vise hele familien kvalitetsindhold, som er passende for de forskellige aldersgrupper. Du er ansvarlig for at sikre, at din app er egnet til børn, og at den overholder alle relevante love, inden du indsender den til programmet For hele familien eller indsender en app, der er rettet mod børn, til Google Play Butik.

Lær om processen for apps til familier, og gennemgå den interaktive tjekliste på App-akademiet.

Udvikling af apps til børn og familier

Brug af teknologi som redskab til at berige familielivet er i konstant vækst, og forældre leder efter sikkert indhold af høj kvalitet, som de kan dele med deres børn. Du udvikler måske dine apps specielt til børn, eller din app tiltrækker muligvis bare deres opmærksomhed. Google Play vil gerne være med til at sikre, at din app er sikker for alle brugere, også familier.

Ordet "børn" kan betyde forskellige ting i forskellige lande og i forskellige sammenhænge. Det er vigtigt, at du kontakter din advokat for at finde ud af, hvilke forpligtelser og/eller aldersbaserede begrænsninger der gælder for din app. Du ved bedst, hvordan din app fungerer, så vi er afhængige af, at du hjælper os med at sikre, at apps i Google Play er sikre for familier.

Apps, der er udviklet specielt til børn, skal deltage i programmet For hele familien. Hvis din app både er målrettet mod børn og ældre målgrupper, kan du stadig deltage i programmet For hele familien. Alle apps, der tilmelder sig programmet For hele familien, er kvalificeret til [programmet Lærergodkendte apps](#), men vi kan ikke garantere, at din app optages i programmet Lærergodkendte apps. Selvom du ikke vil deltage i programmet For hele familien, skal du stadig overholde kravene i Google Plays familierpolitik nedenfor og alle andre [programpolitikker for udviklere i Google Play](#) og [Distributionsaftale for udviklere](#).

Krav til Play Console

[Målgruppe og indhold](#)

I sektionen [Målgruppe og indhold](#) i Google Play Console skal du angive målgruppen for din app forud for udgivelsen ved at vælge fra listen over angivne aldersgrupper. Uanset hvad du angiver i Google Play Console, kan det have indflydelse på Google Plays vurdering af din erklærede målgruppe, hvis du vælger at medtage billeder og terminologi i din app, der kan betragtes som målrettet mod børn. Google Play forbeholder sig ret til at foretage sin egen gennemgang af de angivne oplysninger om appen for at afgøre, om den oplyste målgruppe er korrekt.

Hvis du vælger en målgruppe, der kun omfatter voksne, men Google fastslår, at dette er unøjagtigt, fordi din app både henvender sig til børn og voksne, får du mulighed for at tydeliggøre for brugerne, at din app ikke er rettet mod børn, ved at acceptere at vise en advarselsetiket.

Du bør kun vælge mere end én aldersgruppe som målgruppe for din app, hvis du har udviklet appen til brugere inden for de valgte aldersgrupper og sørget for, at den er egnet til disse aldersgrupper. Aldersgruppen "For børn op til 5 år" bør f.eks. kun være valgt som aldersmålgruppe for apps, der er udviklet til babyer, småbørn og børn i førskolealderen. Hvis din app er udviklet til et bestemt klassetrin, skal du vælge den aldersgruppe, der bedst repræsenterer det pågældende klassetrin. Du bør kun vælge aldersgrupper, der omfatter både børn og voksne, hvis appen reelt er udviklet til brugere i alle aldre.

Opdateringer af sektionen Målgruppe og indhold

Du kan altid opdatere oplysningerne om din app i sektionen Målgruppe og indhold i Google Play Console. Der kræves en [appopdatering](#), før disse oplysninger afspejles i Google Play Butik. Eventuelle ændringer, du foretager i denne sektion af Google Play Console, kan blive gennemgået med henblik på overholdelse af politikken, selv før en appopdatering indsendes.

Vi anbefaler kraftigt, at du giver dine eksisterende brugere besked, hvis du ændrer aldersmålgruppen for din app eller begynder at bruge annoncer eller køb i appen. Dette kan du gøre enten ved at bruge afsnittet "Hvad er nyt" på siden med din apps butiksfortegnelse eller via notifikationer i appen.

Urigtige oplysninger i Play Console

Urigtige oplysninger om din app i Play Console, herunder sektionen Målgruppe og indhold, kan medføre fjernelse eller suspendering af din app, så det er vigtigt at angive nøjagtige oplysninger.

Krav til familiepolitik

Hvis en af målgrupperne for din app er børn, skal du opfylde følgende krav. Manglende opfyldelse af disse krav kan resultere i fjernelse eller suspendering af appen.

1. **Appindhold:** Indhold i din app, der er tilgængeligt for børn, skal være egnet til børn.
2. **Svar i Google Play Console:** Du skal svare nøjagtigt på spørgsmålene i Google Play Console vedrørende din app og opdatere svarene, så de nøjagtigt afspejler eventuelle ændringer i din app.
3. **Annoncer:** Hvis din app viser annoncer til børn eller brugere af ukendt alder, skal du gøre følgende:
 - Brug kun [Google Play-certificerede annonce-SDK'er](#) til at vise annoncer til disse brugere
 - Sørg for, at annoncer, der vises til disse brugere, ikke anvender interessebaseret annoncering (annoncering, der er målrettet mod individuelle brugere med bestemte karakteristika baseret på deres onlinebrowsingadfærd) eller remarketing (annoncering, der er målrettet mod individuelle brugere baseret på tidligere interaktion med en app eller et website)
 - Sørg for, at annoncer, der vises til disse brugere, omfatter indhold, der er passende for børn.
 - Sørg for, at annoncer, der vises til disse brugere, følger kravene til annonceformat for familier.
 - Sørg for, at din app overholder alle gældende lovbestemmelser og branchestandarder vedrørende annoncering til børn.
4. **Dataindsamling:** Du skal oplyse, om du indsamler [personlige og følsomme oplysninger](#) fra børn i din app, herunder via API'er og SDK'er, der kaldes eller bruges i din app. Følsomme oplysninger fra børn omfatter, men er ikke begrænset til, godkendelsesoplysninger, data fra mikrofon og kamerasensor, enhedsdata, Android-id, brugsdata om annoncer og annoncerings-id.
5. **API'er og SDK'er:** Du skal sørge for, at din app implementerer API'er og SDK'er korrekt.
 - Apps, der udelukkende er rettet mod børn, må ikke indeholde API'er eller SDK'er, der ikke er godkendt til brug i børneorienterede tjenester. Dette omfatter Login med Google (eller andre Google API-tjenester, der har adgang til data, som er tilknyttet en Google-konto), Spiltjenester i Google Play samt alle andre API-tjenester, der anvender OAuth-teknologi til godkendelse og tilladelse.
 - Apps, der er rettet mod både børn og ældre målgrupper, må ikke implementere API'er eller SDK'er, som ikke er godkendt til brug i tjenester, der er rettet mod børn, medmindre de anvendes bag en [neutral aldersskærm](#) eller implementeres på en måde, som ikke resulterer i indsamling af data fra børn (f.eks. ved brug af Login med Google som en valgfri funktion). Apps, der både er målrettet mod børn og ældre målgrupper, må ikke kræve, at brugere logger ind eller får adgang til appindhold via en API eller SDK, der ikke er godkendt til brug i tjenester, der er rettet mod børn.
6. **Privatlivspolitik:** Du skal angive et link til din apps privatlivspolitik på din apps profilside i Play Butik. Dette link skal til enhver tid vedligeholdes, så længe appen er tilgængelig i butikken, og det skal linke til en privatlivspolitik, som nøjagtigt beskriver, hvordan din app indsamler og bruger data.
7. **Særlige begrænsninger:**
 - Hvis din app anvender augmented reality, skal du vise en sikkerhedsadvarsel, så snart AR-sektionen åbnes. Advarslen skal indeholde følgende:
 - En passende meddelelse om vigtigheden af forældreopsyn.
 - En påmindelse om at være opmærksom på fysiske farer i den virkelige verden (f.eks. "Vær opmærksom på dine omgivelser").
 - Din app må ikke kræve brug af en enhed, der anbefales til ikke at blive brugt af børn (f.eks. Daydream og Oculus).
8. **Overholdelse af lovgivningen:** Du skal sørge for, at din app og de API'er og SDK'er, som din app kalder eller anvender, overholder [den amerikanske Children's Online Privacy and Protection Act \(COPPA\)](#), [EU's persondataforordning \(GDPR\)](#) og alle andre gældende love og bestemmelser.

Her er nogle eksempler på typiske overtrædelser:

- Apps, der promoverer spil til børn på deres profilside i Play Butik, men hvor appens indhold kun er egnet til voksne.
- Apps, der implementerer API'er med servicevilkår, som forbyder brug i apps, der er rettet mod børn.
- Apps, der forherliger brug af alkohol, tobak eller regulerede stoffer.
- Apps, der omfatter ægte eller simuleret hasardspil.
- Apps, der indeholder vold, lemlæstelse eller chokerende indhold, som er uegnet for børn.
- Apps, der leverer datingtjenester eller tilbyder rådgivning om sex eller ægteskab.

- Apps, der indeholder links til websites, som omfatter indhold, der overtræder Google Plays [programpolitikker for udviklere](#).
- Apps, der viser annoncer med voksenindhold (f.eks. voldeligt indhold, seksuelt indhold eller indhold med hasardspil) til børn. Se [politikkerne om familieannoncer og indtægtsgenerering](#) for at få flere oplysninger om Google Plays politikker for annoncering, køb i apps og kommercielt indhold målrettet børn.

Programmet For hele familien

Apps, der er udviklet specielt til børn, skal deltage i programmet For hele familien. Hvis din app er udviklet til alle, herunder børn og familier, kan du også ansøge om at deltage i programmet.

Før din anmodning om deltagelse i programmet kan accepteres, skal din app overholde alle kravene i familiepolicikken og kvalifikationskravene til For hele familien samt de krav, der er angivet i [programpolitikkerne for udviklere i Google Play](#) og [Distributionsaftale for udviklere](#).

Klik [her](#) for at få flere oplysninger om indsendelse af din app til optagelse i programmet.

Kvalifikation til programmet

Alle apps, der deltager i programmet For hele familien, skal have både app- og annonceindhold, der er relevant og passende for børn, og skal opfylde alle kravene nedenfor. Apps, der optages i programmet For hele familien, skal til enhver tid overholde alle programkravene. Google Play kan afvise, fjerne eller suspendere apps, som vi vurderer til at være upassende til programmet For hele familien.

Krav til For hele familien

1. Apps skal have ESRB-klassificeringen "Everyone" (Alle) eller "Everyone 10+" (Alle fra 10 år) eller tilsvarende.
2. Du skal nøjagtigt oplyse appens interaktive elementer på spørgeskemaet for indholdsklassificering i Google Play Console, og om:
 - Brugere kan interagere eller udveksle oplysninger.
 - Din app deler personlige oplysninger, som brugerne har udleveret, med tredjeparter.
 - Din app deler brugerens fysiske placering med andre brugere.
3. Hvis din app benytter [Android Speech API](#), skal appens RecognizerIntent.EXTRA_CALLING_PACKAGE angives til dens PackageName.
4. Apps må kun anvende [Google Play-certificerede annonce-SDK'er](#).
5. Apps, der er udviklet specielt til børn, må ikke anmode om adgangstilladelser til placering.
6. Apps skal anvende [CDM \(Companion Device Manager\)](#) ved anmodning om Bluetooth, medmindre appen kun er målrettet mod versioner af operativsystemer, der ikke er kompatible med CDM.

Her er nogle eksempler på almindelige apps, der ikke er kvalificeret til programmet:

- Apps, der har ESRB-klassificeringen Alle, men indeholder annoncer for hasardspil
- Apps til forældre eller omsorgsgivere (f.eks. registrering af amning, udviklingsvejledning)
- Forældrevejledninger eller apps til enhedsadministration, som kun er beregnet til brug af forældre eller omsorgsgivere
- Apps, der anvender et appikon eller starterikon, der er upassende for børn

Kategorier

Hvis du bliver godkendt til at deltage i programmet For hele familien, kan du vælge en anden familiespecifik kategori, der beskriver din app. Disse kategorier er tilgængelige for apps, der deltager i programmet For hele familien:

Action og eventyr: Actionprægede apps/spil, herunder alt fra simple racerspil til eventyrspil og andre apps og spil, der er udviklet til at skabe spænding.

Hjernegymnastik: Spil, der får brugeren til at tænke, herunder nørklespil, vendespil, quizzes og andre spil, der udfordrer hukommelsen, intelligensen eller logikken.

Kreativitet: Apps og spil af kreativ karakter som f.eks. apps til tegning, maling og kodning og andre apps og spil, hvor brugeren kan bygge og skabe ting.

Uddannelse: Apps og spil, der er udviklet med input fra læringseksperter (f.eks. undervisere, læringsspecialister og forskere) med henblik på at fremme læring, herunder akademisk, socio-emotionel, fysisk og kreativ læring samt læring med relation til grundlæggende livsfærdigheder, kritisk tænkning og problemløsning.

Musik og video: Apps og spil med en musikalsk komponent eller en videokomponent, bl.a. apps til instrumentsimulation og apps, der leverer lydindhold med video og musik.

Rolleleg: Apps og spil, hvor brugeren kan påtage sig en rolle, f.eks. lege kok, omsorgsgiver, prins/prinsesse, brandmand, politibetjent eller en fiktiv figur.

Annoncer og indtægtsgenerering

Politikkerne nedenfor gælder for enhver form for annoncering i din app, herunder annoncer for dine apps og tredjepartsapps, tilbud om køb i appen eller andet kommercielt indhold (som f.eks. betalt produktplacering), der vises til brugere af apps, som er underlagt kravene i familierpolitikken og/eller kravene for programmet For hele familien. Alle annoncer, tilbud om køb i appen og kommercielt indhold i disse apps skal desuden overholde alle gældende love og bestemmelser (herunder relevante retningslinjer for selvregulering eller for branchen).

Google Play forbeholder sig retten til at afvise, fjerne eller suspendere apps, der anvender alt for aggressive forretningsmetoder.

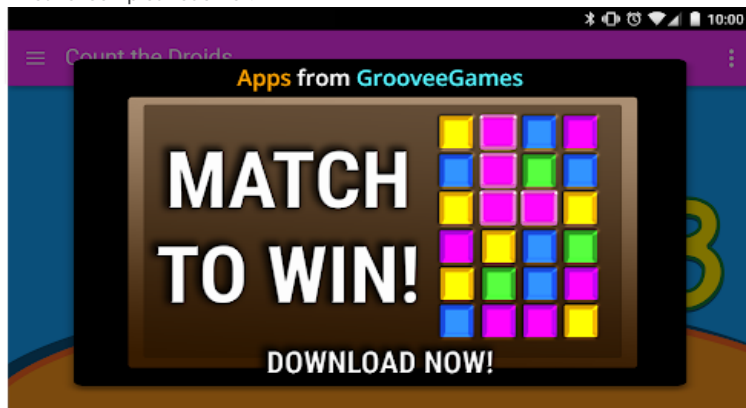
Krav til annonceformat

Annoncer og tilbud om køb i appen må ikke have vildledende indhold eller være udformet på en måde, som resulterer i utilsigtede klik fra børnebrugere. Følgende er ikke tilladt:

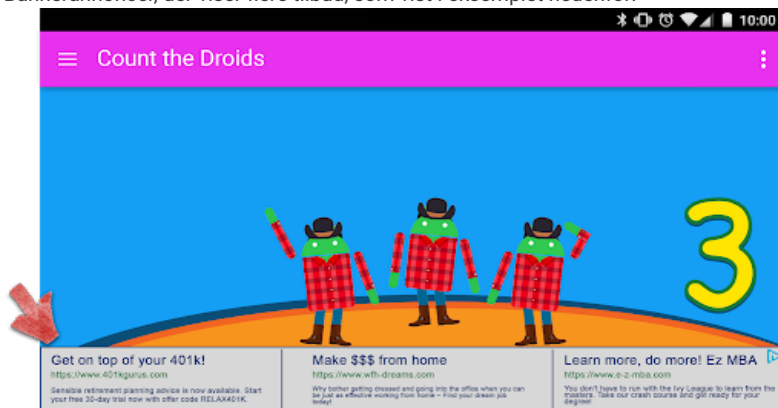
- Forstyrrende annoncer, herunder annoncer, der fylder hele skærmen eller forstyrrer normal brug, og som ikke tydeligt angiver, hvordan annoncen kan afvises (f.eks. [annoncevægge](#))
- Annoncer, som forhindrer normal brug af appen eller spillet og ikke kan lukkes efter fem sekunder Annoncer, der ikke forstyrrer normal brug af appen eller spillet, må vises i mere end fem sekunder (f.eks. videoindhold med integrerede annoncer).
- Mellemliggende annoncer eller tilbud om køb i appen, der vises umiddelbart efter, at appen åbnes
- Flere annonceplaceringer på en side (f.eks. bannerannoncer, der viser flere tilbud på én placering eller viser mere end én banner- eller videoannonce, er ikke tilladt).
- Annoncer eller tilbud om køb i appen, der ikke klart kan skelnes fra dit appindhold
- Brug af chokerende eller følelsesmæssigt manipulerende taktik for at tilskynde brugere til at se annoncer eller foretage køb i appen
- Manglende angivelse af, hvornår der er tale om brug af virtuelle spilmonter og virkelige penge til at foretage køb i appen

Her er nogle eksempler på typiske overtrædelser af annonceformatet

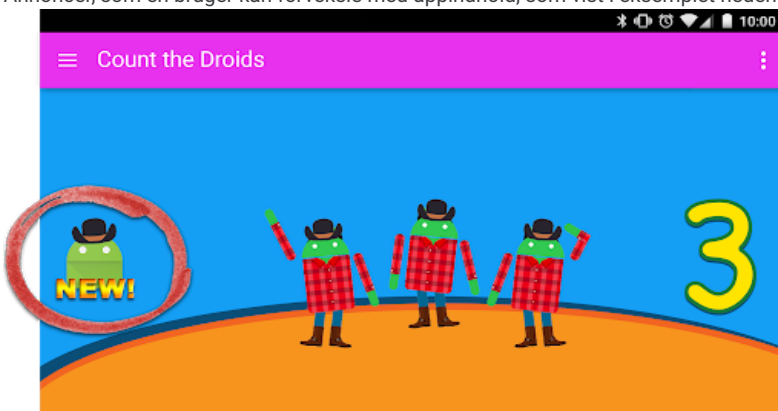
- Annoncer, der bevæger sig væk fra en brugers finger, når brugeren forsøger at lukke den
- Annoncer, der fylder det meste eller hele enhedens skærm uden at give brugeren en åbenlys måde at fjerne den på, som vist i eksemplet nedenfor:



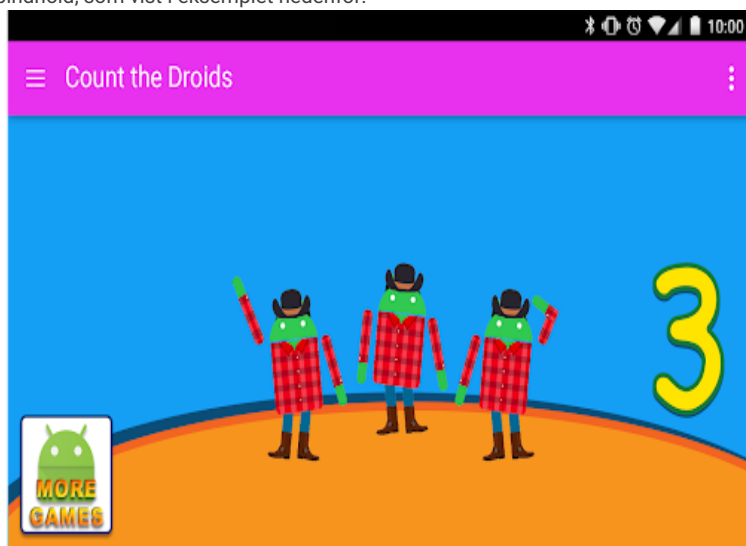
- Bannerannoncer, der viser flere tilbud, som vist i eksemplet nedenfor:



- Annoncer, som en bruger kan forveksle med appindhold, som vist i eksemplet nedenfor:



- Knapper eller annoncer, der promoverer dine andre profilsider i Google Play Butik, men som ikke kan skelnes fra appindhold, som vist i eksemplet nedenfor:



Her er nogle eksempler på upassende annonceindhold, der ikke bør vises til børn.

- Upassende medieindhold:** Annoncer for tv-serier, film, musikalbum eller enhver anden medieform, som er uegnet for børn.
- Upassende videospil og software, der kan downloades:** Annoncer for software, der kan downloades, og elektroniske videospil, der ikke er passende for børn.
- Receptpligtig medicin eller skadelige stoffer:** Annoncer for alkohol, tobak, regulerede stoffer eller andre skadelige stoffer.
- Hasardspil:** Annoncer for simuleret hasardspil, konkurrencer eller lotterier, også selv om det er gratis at deltage.

Voksenindhold og seksuelt orienteret indhold: Annoncer med seksuelt eller seksuelt orienteret indhold og indhold, der

- er uegnet for børn.
- **Dating eller forhold:** Annoncer for datingwebsites eller websites til voksenforhold.
- **Voldeligt indhold:** Annoncer med voldeligt og udpenslet indhold, som er uegnet for børn.

Annonce-SDK'er

Hvis du viser annoncer i din app, og din målgruppe kun omfatter børn, skal du bruge [Google Play-certificerede annonce-SDK'er](#). Hvis målgruppen for din app omfatter både børn og ældre brugere, skal du implementere metoder til aldersbekræftelse, f.eks. en [neutral aldersskærm](#), og sørge for, at de annoncer, der vises til børn, udelukkende stammer fra Google Play-certificerede annonce-SDK'er. Det er et krav, at apps i programmet For hele familien kun bruger selvcertificerede annonce-SDK'er.

Gå til siden med [politikken for Program for annoncer til børn](#) for at få flere oplysninger om disse krav og for at se den aktuelle liste over godkendte annonce-SDK'er.

Hvis du bruger AdMob, henviser vi til [Hjælp til AdMob](#) for flere oplysninger om deres produkter.

Det er dit ansvar at sikre, at din app opfylder alle krav vedrørende annoncer, køb i appen og kommercielt indhold. Kontakt udbyderen af din annonce-SDK for at få flere oplysninger om deres indholdspolitikker og annoncepraksis.

Køb i apps

Google Play godkender alle brugere igen inden køb i apps, der deltager i programmet For hele familien. Denne foranstaltning er med til at sikre, at køb godkendes af en økonomisk ansvarlig part og ikke af børn.

Håndhævelse

Det er altid bedre at undgå at overtræde en politik, end det er at håndtere en overtrædelse. Men når en politik overtrædes, gør vi vores bedste for at sikre, at udviklere forstår, hvordan de kan få deres app til at overholde politikken. Du er velkommen til at kontakte os, hvis du [oplever overtrædelser](#) eller har spørgsmål om [håndtering af overtrædelser](#).

Politikkens dækning

Vores politikker gælder for alt indhold, som din app viser eller linker til, herunder alle annoncer, som vises til brugerne, og alt brugergenereret indhold, der vises eller linkes til. Derudover gælder de for alt indhold fra din udviklerkonto, som er offentligt tilgængeligt i Google Play, herunder udviklernavn og landingsside for det anførte udviklerwebsite.

Vi tillader ikke apps, der giver brugerne mulighed for at installere andre apps på deres enheder. Apps, der giver adgang til andre apps, spil eller software uden installation, herunder funktioner og oplevelser fra tredjeparter, skal sikre, at alt indhold, de giver adgang til, overholder alle [Google Play-politikker](#). De kan desuden blive underlagt yderligere gennemgang for at sikre, at de er i overensstemmelse med vores politikker.

De udtryk, der er defineret i disse politikker, har samme betydning som i [Distributionsaftale for udviklere](#) (DDA, Developer Distribution Agreement). Ud over at overholde disse politikker og DDA-aftalen skal indholdet af din app også klassificeres i overensstemmelse med vores [retningslinjer for indholdsklassificering](#).

Ved vurderingen af, om apps skal medtages eller fjernes fra Google Play, tager vi en række faktorer i betragtning, herunder, men ikke begrænset til, et skadeligt adfærdsmønster og en stor risiko for misbrug. Vi identificerer risikoen for misbrug, herunder, men ikke begrænset til, elementer såsom tidligere overtrædelser, brugerfeedback og brug af populære brands, figurer og andre aktiver.

Sådan fungerer Google Play Protect

Google Play Protect tjekker apps, når du installerer dem. Tjenesten scanner også jævnlige enheden. Hvis der registreres en potentielt skadelig app, kan Play Protect gøre følgende:

- Sendt dig en notifikation. Tryk på notifikationen og derefter på Afinstaller for at fjerne appen.
- Deaktivere appen, indtil du afinstallerer den.
- Fjerne appen automatisk. Hvis der registreres en skadelig app, får du i de fleste tilfælde en notifikation om, at appen er fjernet.

Sådan fungerer malwarebeskyttelse

Google kan modtage oplysninger om følgende for at beskytte dig mod skadelig software fra tredjeparter, skadelige webadresser og andre sikkerhedsproblemer:

- Din enheds netværksforbindelser
- Potentielt skadelige webadresser
- Operativsystemet og apps, der er installeret på din enhed via Google Play eller andre kilder.

Du får muligvis en advarsel fra Google om en app eller en webadresse, der kan være usikker. Installationen af appen eller webadressen kan blive fjernet eller blokeret af Google, hvis den er kendt for at skade enheder, data eller brugere.

Du kan vælge at deaktivere nogle af disse beskyttelsesmetoder i indstillingerne på din enhed. Google kan dog fortsætte med at modtage oplysninger om apps, der er installeret via Google Play. Apps, der er installeret på din enhed via andre kilder, kan desuden fortsat blive undersøgt for sikkerhedsproblemer, uden at der sendes oplysninger til Google.

Sådan fungerer advarsler om beskyttelse af personlige oplysninger

Google Play Protect underretter dig, hvis en app fjernes fra Google Play Butik, fordi appen kan tilgå dine personlige oplysninger, og du får mulighed for at afinstallere appen.

Håndhævelsesproces

Hvis din app overtræder nogen af vores politikker, træffer vi de nødvendige foranstaltninger som beskrevet nedenfor. Derudover sender vi dig en mail med relevante oplysninger om den handling, vi har foretaget, og en vejledning i, hvordan du appellerer, hvis du mener, at vores handling er fejlagtig.

Bemærk, at det ikke er sikkert, at alle overtrædelser af politikker i din app eller dit appkatalog er angivet i meddelelsen om fjernelse eller andre administrative meddelelser. Udviklerne er ansvarlige for at reagere på alle problemer med overholdelse af politikker og være ekstra omhyggelige med at sikre, at den resterende del af appen overholder politikken fuldt ud. Hvis du ikke løser problemer med overtrædelse af politikker i alle dine apps, kan det resultere i yderligere håndhævelseshandlinger.

Gentagne eller alvorlige overtrædelser (f.eks. malware, bedrageri eller apps, der kan medføre skade på brugere eller enheder) af disse politikker eller af [Distributionsaftale for udviklere](#) vil medføre, at individuelle eller relaterede Google Play-udviklerkonti lukkes.

Håndhævelseshandlinger

Forskellige håndhævelseshandlinger kan påvirke din app på forskellige måder. Den følgende sektion beskriver de forskellige handlinger, som Google Play kan foretage, og deres indvirkning på din app og/eller din Google Play-udviklerkonto. Disse oplysninger forklares også i [denne video](#).

Afvisning

- En ny app eller appopdatering, der indsendes til gennemgang, bliver ikke gjort tilgængelig i Google Play.
- Hvis en opdatering til en eksisterende app blev afvist, forbliver den appversion, der blev udgivet før opdateringen, tilgængelig i Google Play.
- Afvisninger påvirker ikke din adgang til en afvist apps eksisterende brugerinstallationer, statistik og bedømmelser.
- Afvisninger påvirker ikke din udviklerkontos omdømme i Google Play.

Bemærk! Forsøg ikke at genindsende en afvist app, før du har håndteret alle overtrædelser af politikker.

Fjernelse

- Appen fjernes fra Google Play sammen med eventuelle tidligere versioner af den pågældende app, og brugerne kan ikke længere downloade den.
- Da appen er fjernet, kan brugerne ikke se appens profilside i Play Butik, brugerinstallationer, statistik og bedømmelser. Disse oplysninger gendannes, når du har indsendt en opdatering af den fjernede app, der overholder alle politikker.
- Brugere kan muligvis ikke foretage køb i appen eller benytte faktureringsfunktioner i appen, før en version, der overholder politikken, er godkendt af Google Play.
- Fjernelser påvirker ikke din Google Play-udviklerkontos omdømme med det samme, men flere fjernelser kan medføre suspendering.

Bemærk! Forsøg ikke at genudgive en fjernet app, før du har håndteret alle overtrædelser af politikker.

Suspendering

- Appen fjernes fra Google Play sammen med eventuelle tidligere versioner af den pågældende app, og brugerne kan ikke længere downloade den.

- Grove eller gentagne overtrædelser af politikker kan medføre suspendering. Det samme gælder for gentagne afvisninger eller fjernelser af apps.
- Da appen er suspenderet, kan brugerne ikke se appens profilside i Play Butik, eksisterende brugerinstallationer, statistik og bedømmelser. Disse oplysninger gendannes, når du har indsendt en opdatering af den fjernede app, der overholder alle politikker.
- Du kan ikke længere bruge en suspenderet apps APK-fil eller app-pakke.
- Brugerne kan ikke foretage køb i appen eller benytte faktureringsfunktioner i appen, før en version, der overholder politikken, er godkendt af Google Play.
- Suspenderinger har en negativ indvirkning på din udviklerkontos omdømme i Google Play. Flere negative hændelser kan medføre lukning af individuelle og relaterede Google Play-udviklerkonti.

Bemærk! Forsøg ikke at udgive en suspenderet app igen, medmindre Google Play har meddelt, at du må gøre det.

Begrænset synlighed

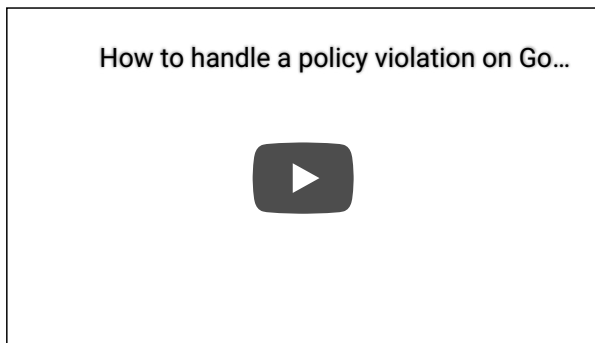
- Din apps synlighed i Google Play er begrænset. Din app forbliver tilgængelig i Google Play, og brugerne kan få adgang til den via et direkte link til appens profilside i Play Butik.
- Det påvirker ikke din udviklerkontos omdømme i Google Play, at din app er i tilstanden med begrænset synlighed.
- Når din app er i tilstanden med begrænset synlighed, påvirker det ikke brugernes mulighed for at se appens eksisterende profilside i Play Butik, brugerinstallationer, statistik og bedømmelser.

Kontrolukning

- Hvis din udviklerkonto lukkes, bliver alle apps i dit katalog fjernet fra Google Play, og du kan ikke længere udgive nye apps. Dette indebærer, at relaterede Google Play-udviklerkonti også suspenderes permanent.
- Gentagne eller grove overtrædelser af politikker kan også medføre lukning af din Play Console-konto.
- Da de apps, der er tilknyttet den lukkede konto, bliver fjernet, kan brugerne ikke se appenes profilsider i Play Butik, eksisterende brugerinstallationer, statistik og bedømmelser.

Bemærk! Alle nye konti, du forsøger at åbne, lukkes også (uden refusion af tilmeldingsgebyret for udviklere), så du skal ikke forsøge at oprette en ny konto i Play Console, mens en af dine andre konti er lukket.

Håndtering og rapportering af overtrædelser af politikker



Appel af en håndhævelseshandling

Vi genindsætter apps, hvis der er sket en fejl, og vi afgør, at din app ikke overtræder programpolitikkerne for Google Play og Distributionsaftale for udviklere. Hvis du har gennemgået politikkerne omhyggeligt og mener, at vores beslutning kan være en fejl, skal du følge vejledningen i den notifikation, du modtager via mail, for at appellere vores beslutning.

Yderligere ressourcer

Hvis du har brug for flere oplysninger om en håndhævelseshandling eller en bedømmelse/kommentar fra en bruger, kan du se nogle af nedenstående ressourcer eller kontakte os via [Hjælp til Google Play](#). Vi kan dog ikke tilbyde dig juridisk bistand. Hvis du har behov for juridisk bistand, bedes du rådføre dig med en advokat.

- [Appbekræftelse og appeller](#)
- [Rapportér om overtrædelse af politikker](#)
- [Kontakt Google Play om lukning af en konto eller fjernelse af en app](#)
- [Advarsler](#)
- [Rapportér upassende apps og kommentarer](#)

- [Min app er blevet fjernet fra Google Play](#)
- [Sådan fungerer lukning af Google Play-udviklerkonti](#)



Send feedback om denne artikel

Var disse oplysninger nyttige?

Ja

Nej

Har du brug for mere hjælp?

Prøv følgende næste trin:

Kontakt os

Fortæl os mere, så hjælper vi dig videre