

Google Developer Policy - April 16, 2020

Usilujme společně o nejdůvěryhodnější zdroj aplikací a her

Motorem našeho společného úspěchu jsou vaše inovace, ale s úspěchem přichází i odpovědnost. Tyto programové zásady pro vývojáře společně s [distribuční smlouvou pro vývojáře](#) zajišťují, že budeme prostřednictvím Google Play společně nabízet nejinovativnější a nejdůvěryhodnější aplikace na světě více než miliardě uživatelů. Naše zásady si můžete prohlédnout níže nebo ve [verzi pro tisk](#).

Zakázaný obsah

Pomocí Google Play denně vyhledávají aplikace a hry lidé z celého světa. Před publikováním aplikace se zeptejte sami sebe, zda je aplikace pro Google Play vhodná a zda dodržuje místní zákony.

Ohrožení dětí

Aplikace s obsahem, který sexualizuje nezletilé, budou z obchodu ihned odstraněny. Nejsou povoleny aplikace, které jsou přitažlivé pro děti, ale obsahují motivy jen pro dospělé.

Pokud se dozvíme o obsahu, který zobrazuje sexuální zneužívání dětí, nahlásíme to příslušným orgánům a smažeme účty Google uživatelů zapojených do distribuce.

Aby platforma Google Play zůstala bezpečná a zdvořilá, vytvořili jsme standardy, které definují a zakazují obsah škodlivý nebo nevhodný pro uživatele.

Aby platforma Google Play zůstala bezpečná a zdvořilá, vytvořili jsme standardy, které definují a zakazují obsah škodlivý nebo nevhodný pro uživatele.

Sexuální obsah

Nepovolujeme aplikace, které zahrnují či propagují sexuální obsah (např. pornografii), ani obsah a služby určené k uspokojování sexuálních potřeb. Obsah zahrnující nahotu může být povolen v případě, že má primárně vzdělávací, dokumentární, vědecký či umělecký účel a nahota v něm není bezdůvodná.

Aby platforma Google Play zůstala bezpečná a zdvořilá, vytvořili jsme standardy, které definují a zakazují obsah škodlivý nebo nevhodný pro uživatele.

Vyobrazení nahých nebo jen minimálně oblečených osob v prostředí, kde by takové oblečení ve veřejném kontextu nebylo přijatelné.
Vyobrazení, animace nebo ilustrace sexuálních aktivit nebo sexuálně sugestivních póz.
Obsah zobrazující sexuální pomůcky a fetiše.
Obscenní či sprostý obsah.
Obsah, který zobrazuje, popisuje nebo propaguje zoofilii.
Aplikace, které propagují sexuální zábavu, eskortní služby nebo jiné služby, které lze interpretovat jako poskytování sexuálních služeb za peníze.

Nenávistné výroky

Nepovolujeme aplikace, které propagují násilí nebo podněcují k nenávisti vůči určitým osobám nebo skupinám na základě rasového nebo etnického původu, náboženství, postižení, věku, národnosti, statusu veterána, sexuální orientace, pohlaví, genderové identity ani jakékoliv jiné charakteristiky spojené se systematickou diskriminací nebo marginalizací.
Aby platforma Google Play zůstala bezpečná a zdvořilá, vytvořili jsme standardy, které definují a zakazují obsah škodlivý nebo nevhodný pro uživatele.

Kompilace tvrzení, které mají za cíl ukázat, že je určitá chráněná skupina nelidská, podřadná nebo si zaslouhuje nenávit.
Aplikace s teoriemi, že příslušníci určité chráněné skupiny mají negativní vlastnosti (např. že jsou zákešní, zkažení, zlí apod.), nebo explicitními či implicitními tvrzeními, že taková skupina představuje hrozbu.
Obsah nebo projevy, které se ostatní lidi pokouší přesvědčit k nenávisti nebo diskriminaci vůči členům chráněné skupiny.

Násilí

Nepovolujeme aplikace, které zobrazují bezdůvodné násilí či jiné nebezpečné aktivity, ani obsah, který takovému chování napomáhá.
Aby platforma Google Play zůstala bezpečná a zdvořilá, vytvořili jsme standardy, které definují a zakazují obsah škodlivý nebo nevhodný pro uživatele.

Grafické znázornění nebo popis realistického násilí nebo násilných hrozeb vůči člověku nebo zvířeti.
Aplikace, které propagují sebepoškozování, sebevraždy, poruchy příjmu potravy, hry spojené s dušením nebo jiné aktivity spojené s rizikem vážného zranění nebo úmrtí.

Teroristický obsah

Teroristickým organizacím nedovolujeme publikovat na Google Play aplikace k žádným účelům, ani k náboru členů.

Nepovolujeme aplikace, jejichž obsah souvisí s terorismem, například podněcuje k teroristickým činům či násilí nebo oslavuje teroristické útoky. Pokud sdílíte obsah související s terorismem ve

vzdělávacím, dokumentárním, vědeckém nebo uměleckém kontextu, vždy k němu poskytněte dostatek informací, abyste ho uživatelům pomohli pochopit.

Citlivé události

Nepovolujeme aplikace, které postrádají přiměřenou ohleduplnost k přírodním katastrofám, krutým činům, konfliktům, úmrtím nebo jiným tragickým událostem, ani aplikace, které z takovýchto událostí těží.

Aby platforma Google Play zůstala bezpečná a zdvořilá, vytvořili jsme standardy, které definují a zakazují obsah škodlivý nebo nevhodný pro uživatele.

Nedostatek ohleduplnosti ohledně smrti skutečné osoby nebo skupiny lidí následkem sebevraždy, předávkování, přirozených příčin apod.

Popírání závažné tragické události.

Vystupování za účelem profitování z tragické události bez zřejmého užitku pro oběti.

Šikana a obtěžování

Nepovolujeme aplikace, které obsahují hrozby nebo uživatele obtěžují či zastrašují, ani aplikace, které takové chování podporují.

Aby platforma Google Play zůstala bezpečná a zdvořilá, vytvořili jsme standardy, které definují a zakazují obsah škodlivý nebo nevhodný pro uživatele.

Šikanování obětí mezinárodních nebo náboženských konfliktů.

Obsah, který se snaží ostatní zneužívat, včetně vydírání, vyhrožování apod.

Zveřejňování obsahu za účelem veřejného ponížení určité osoby.

Obtěžování obětí tragických událostí nebo jejich přátel a rodiny.

Nebezpečné produkty

Nepovolujeme aplikace, které umožňují prodej výbušnin, střelných zbraní, střeliva a některého příslušenství střelných zbraní.

Zakázáno je příslušenství, pomocí něhož lze u zbraní napodobit automatickou střelbu nebo zbraně přestavět na automatické (například urychlovače střelby typu bump stock, gatling trigger, drop-in auto sears a různé sady na přestavbu), a také zásobníky nebo pásy na více než 30 nábojů.

Nepovolujeme aplikace, které poskytují návody k výrobě výbušnin, střelných zbraní, střeliva, zakázaného příslušenství střelných zbraní nebo jiných typů zbraní. Týká se to mimo jiné i návodů k přestavbě střelných zbraní na automatické nebo k napodobení automatické střelby.

Marihuana

Bez ohledu na legálnost nepovolujeme aplikace, které umožňují prodej marihuany nebo marihuanových produktů.

Aby platforma Google Play zůstala bezpečná a zdvořilá, vytvořili jsme standardy, které definují a zakazují obsah škodlivý nebo nevhodný pro uživatele.

Umožnění objednávek marihuany prostřednictvím nákupního košíku v aplikaci.
Pomáhání uživatelům s dohodnutím dodávky nebo vyzvednutí marihuany.
Umožňování prodeje produktů s obsahem THC.

Tabákové výrobky a alkohol

Nepovolujeme aplikace, které umožňují prodej tabákových výrobků (včetně elektronických cigaret) nebo podporují nezodpovědnou konzumaci alkoholu či tabákových výrobků. Aby platforma Google Play zůstala bezpečná a zdvořilá, vytvořili jsme standardy, které definují a zakazují obsah škodlivý nebo nevhodný pro uživatele.

Vyobrazení nebo propagace konzumace alkoholu či tabáku nezletilými nebo prodeje těchto produktů nezletilým.

Naznačování, že konzumace tabákových výrobků může zlepšit společenský, sexuální, profesionální, intelektuální či tělesný stav.

Pozitivní prezentace nadměrného pití, včetně zobrazování nadměrného a nestřídmého pití či závodů v pití v pozitivním světle.

Finanční služby

Nepovolujeme aplikace, které uživatele vystavují klamavým nebo škodlivým finančním produktům či službám.

Pro účely těchto zásad definujeme finanční produkty a služby jako takové, které souvisejí se správou a investováním peněz a kryptoměn, včetně individuálního poradenství.

Pokud vaše aplikace obsahuje nebo propaguje finanční produkty a služby, musíte splnit státní a místní předpisy všech oblastí a zemí, na které aplikace cílí. (Musíte například zahrnout konkrétní zveřejnění vyžadovaná místními právními předpisy.)

Binární opce

Nepovolujeme aplikace, které uživatelům umožňují obchodovat s binárními opcemi.

Kryptoměny

Nepovolujeme aplikace, které na zařízeních těží kryptoměny. Aplikace pro vzdálenou správu těžby kryptoměn jsou však povoleny.

Osobní půjčky

Osobní půjčky definujeme jako jednorázové finanční půjčky poskytované osobami, organizacemi či subjekty jednotlivým spotřebitelům, jejichž účelem není financování nákupu dlouhodobého majetku ani vzdělání. Spotřebitelé, kteří se zajímají o osobní půjčky, potřebují informace o kvalitě, charakteristikách, poplatcích, rizicích a výhodách produktů zahrnujících půjčky, aby se mohli kvalifikovaně rozhodnout, zda nabídku půjčky využijí.

Příklady: Osobní půjčky, krátkodobé půjčky, peer-to-peer úvěry, zpětné půjčky proti dokladu k vozidlu.

Nepatří sem: Hypotéky, půjčky na automobily, studentské půjčky, revolvingové úvěrové linky (například kreditní karty, osobní úvěrové linky).

Aplikace pro osobní půjčky musejí v metadatech obsahovat následující informace:

minimální a maximální dobu splácení,
maximální roční průměrnou sazbu nákladů (RPSN), která obvykle zahrnuje úrokovou sazbu plus poplatky a další náklady za rok, případně jinou podobnou sazbu vypočtenou v souladu s místními právními předpisy,
reprezentativní příklad celkové ceny půjčky včetně všech souvisejících poplatků.

Nepovolujeme aplikace, které propagují osobní půjčky, u nichž je celou částku nutné splatit do 60 či méně dnů od poskytnutí (tyto půjčky nazýváme „krátkodobé osobní půjčky“). Tato zásada se vztahuje na aplikace, které přímo nabízejí půjčky, oslovují potenciální zákazníky nebo uživatele spojují s externími poskytovateli půjček.

Osobní půjčky s vysokou RPSN

V USA nepovolujeme aplikace pro osobní půjčky, u nichž roční průměrná sazba nákladů (RPSN) činí 36 % nebo více. Aplikace pro osobní půjčky v USA musí uvádět maximální RPSN vypočtenou podle zákona [Truth in Lending Act \(TILA\)](#).

Tato zásada se vztahuje na aplikace, které přímo nabízejí půjčky, oslovují potenciální zákazníky nebo uživatele spojují s externími poskytovateli půjček.

Hazardní hry

Obsah, služby a reklamy usnadňující online hazardní hry povolujeme pouze v případě, že splňují určité požadavky. Povolujeme také aplikace pro denní fantasy sporty, které splňují určité požadavky.

Hazardní aplikace

(V současné době povoleno pouze ve Francii, Irsku a Spojeném království)

Obsah a služby, které umožňují hraní online hazardních her, povolujeme pouze v případě, že jsou splněny následující požadavky:

Aby vývojář mohl distribuovat aplikaci ve službě Play, musí úspěšně dokončit [proces žádosti](#) a musí být přijat.

Aplikace musí splňovat všechny příslušné zákony a oborové standardy ve všech zemích, kde je distribuována.

Vývojář musí mít platnou licenci k provozování hazardních her ve všech zemích, kde je aplikace distribuována.

Aplikace musí zabraňovat nezletilým uživatelům v hraní hazardních her v aplikaci.

Aplikace musí znemožňovat používání v zemích, na které se nevztahuje vývojářova licence k provozování hazardních her.

Aplikace na Google Play NESMÍ být k dispozici ke koupi jako placená a nesmí ani používat fakturaci v aplikaci Google Play.

Aplikace musí být zdarma ke stažení a instalaci z Obchodu.

Aplikace musí mít hodnocení AO (pouze pro dospělé) nebo ekvivalentní hodnocení od organizace IARC.

Aplikace a její záznam v obchodu musí jasně zobrazovat informaci o zodpovědném hraní hazardních her.

V žádných jiných oblastech obsah ani služby umožňující hraní online hazardních her nepovolujeme. Týká se to i internetových kasin, sportovního sázení, loterií a dovednostních her s peněžitými nebo jinými cenami, které mají reálnou hodnotu.

Reklamy na hazardní hry v aplikacích distribuovaných ve službě Play

Reklamy na online hazardní hry povolujeme pouze v případě, že jsou splněny následující požadavky:

Aplikace a reklama (včetně inzerentů hazardních her) musí splňovat všechny příslušné zákony a oborové standardy ve všech oblastech, kde se reklama na hazardní hru zobrazuje.

Reklama musí splňovat místní licenční podmínky pro všechny propagované produkty a služby související s hazardními hrami.

Aplikace nesmí reklamu na hazardní hru zobrazovat osobám, o kterých je známo, že jsou mladší 18 let.

Aplikace nesmí být zařazena do programu Pro celou rodinu.

Aplikace nesmí cílit na osoby mladší 18 let.

Reklama musí na vstupní stránce, v záznamu inzerované aplikace nebo v samotné aplikaci jasně zobrazovat informaci o zodpovědném hraní hazardních her.

Aplikace, která inzeruje reklamu na hazardní hru, nesmí být simulátorem hazardního hraní (zábavní hra, ve které se nehraje o skutečné peníze).

Aby platforma Google Play zůstala bezpečná a zdvořilá, vytvořili jsme standardy, které definují a zakazují obsah škodlivý nebo nevhodný pro uživatele.

Aplikace pro děti s reklamou na služby hazardního hraní.

Aplikace pro denní fantasy sporty (DFS)

Aplikace pro denní fantasy sporty (DFS) povolujeme, pokud splňují následující požadavky:

Aplikace smí umožňovat přístup pouze z USA a smí být distribuována pouze v USA.

Aplikace pro DFS zacílené na jiné jurisdikce než USA musejí projít procesem schválení pro hazardní hry se skutečnými penězi.

Aby vývojář mohl distribuovat aplikaci ve službě Play, musí úspěšně dokončit [proces žádosti pro DFS](#) a musí být přijat.

Aplikace musí splňovat všechny příslušné právní předpisy a oborové standardy ve všech státech nebo územích USA, kde je distribuována.

Vývojář musí mít platnou licenci pro každý stát nebo území USA, kde je pro aplikace pro denní fantasy sporty vyžadována licence.

Aplikace musí zabraňovat nezletilým uživatelům v sázení a provádění peněžních transakcí v aplikaci.

Aplikace musí znemožňovat používání ze států nebo území USA, v nichž vývojář pro aplikace pro denní fantasy sporty nemá potřebnou licenci.

Aplikace musí znemožňovat používání ze států nebo území USA, kde aplikace pro denní fantasy sporty nejsou legální.

Aplikace na Google Play NESMÍ být k dispozici ke koupi jako placená a nesmí ani používat fakturaci v aplikaci Google Play.

Aplikace musí být zdarma ke stažení a instalaci z Obchodu.

Aplikace musí mít hodnocení AO (pouze pro dospělé) nebo ekvivalentní hodnocení od organizace IARC.

Aplikace a její záznam v obchodu musí jasně zobrazovat informaci o zodpovědném hraní hazardních her.

Nezákonné činnosti

Nepovolujeme aplikace, které zprostředkovávají nebo propagují nezákonné činnosti.

Aby platforma Google Play zůstala bezpečná a zdvořilá, vytvořili jsme standardy, které definují a zakazují obsah škodlivý nebo nevhodný pro uživatele.

Zprostředkování prodeje nebo nákupu ilegálních drog nebo léků na předpis bez předpisu.

Vyobrazení konzumace drog, alkoholu či tabáku nezletilými a podpora takového chování.

Návod k pěstování nebo výrobě ilegálních drog.

Obsah vytvářený uživateli

Obsah vytvářený uživateli je obsah, který do aplikace přidávají uživatelé a který je viditelný nebo přístupný minimálně části uživatelů aplikace. Nežádoucí obsah je obsah, který porušuje naše zásady.

Aplikace, které obsahují nebo nabízejí obsah vytvářený uživateli musejí splňovat tyto podmínky:

Musejí zajistit, aby obsah vytvářený uživateli bylo možné vytvářet nebo nahrávat až po přijetí smluvních podmínek nebo uživatelských zásad aplikace.

Musejí způsobem konzistentním s duchem programových zásad služby Google Play pro vývojáře definovat obsah vytvářený uživateli, který je nežádoucí, a musejí jej prostřednictvím svých smluvních podmínek nebo uživatelských zásad zakazovat.

Musejí implementovat robustní, efektivní a průběžné moderování obsahu vytvářeného uživateli, a to způsobem přiměřeným a odpovídajícím typům obsahu vytvářeného uživateli, který je v aplikaci hostován.

V aplikaci musí být k dispozici uživatelsky přívětivý systém k nahlášení a odstranění nežádoucího obsahu vytvářeného uživateli.

V případě aplikací ke streamování přímých přenosů musí být obsah vytvořený uživateli odstraněn, co nejdříve je to přiměřeně možné.

Musejí odebrat přístup uživatelům nebo blokovat uživatele, kteří porušují smluvní podmínky nebo zásady pro uživatele aplikace.

Musejí poskytovat bezpečnostní opatření, která zajistí, aby možnosti zpeněžení v aplikaci nepodporovaly nevhodné chování uživatelů.

Aplikace, jejichž primárním účelem je zprostředkování nežádoucího obsahu vytvářeného uživateli, budou z Google Play odstraněny. Z Google Play budou odstraněny i aplikace, které uživatelé začali používat primárně k hostování nežádoucího obsahu nebo které mezi uživateli získaly pověst míst, kde se takový obsah šíří.

Aby platforma Google Play zůstala bezpečná a zdvořilá, vytvořili jsme standardy, které definují a zakazují obsah škodlivý nebo nevhodný pro uživatele.

Propagace sexuálně explicitního obsahu vytvářeného uživateli, včetně implementace placených funkcí, které uživatele motivují ke sdílení nevhodného obsahu.

Aplikace s obsahem vytvářeným uživateli, které neobsahují dostatečná opatření proti hrozbám, obtěžování nebo šikaně (zejména vůči nezletilým).

Příspěvky, komentáře nebo fotky v aplikaci, jejichž hlavním cílem je obtěžovat uživatele nebo udělat z jiného člověka cíl zneužívání, škodlivého útoku nebo posměchu.

Aplikace, které dlouhodobě neřeší stížnosti uživatelů na nežádoucí obsah.

Neschválené látky

Nepovolujeme aplikace, které propagují nebo prodávají neschválené látky, bez ohledu na prohlášení o legálnosti. Příklady:

Všechny položky v tomto seznamu [zakázaných léčiv a doplňků stravy](#) (který není vyčerpávající).

produkty obsahující rostlinu chvojník,

produkty obsahující lidský hormon choriogonadotropin (hCG) a související s hubnutím či regulací tělesné hmotnosti nebo propagované v kombinaci s anabolickými steroidy, bylinné přípravky a výživové doplňky s aktivními farmaceutickými nebo nebezpečnými složkami,

nepravdivá nebo zavádějící tvrzení týkající se zdraví včetně tvrzení, která naznačují, že je daný výrobek stejně účinný jako léky na předpis či regulované látky,

oficiálně neschválené produkty uváděné na trh způsobem, který naznačuje, že jsou bezpečné nebo účinné při prevenci či léčbě konkrétních nemocí nebo zdravotních obtíží, produkty, na které se vztahují státní nebo regulační opatření či varování,

výrobky s matoucími názvy, které připomínají neschválená léčiva, doplňky stravy či regulované látky.

Další informace o monitorovaných neschválených či zavádějících léčivech a doplňcích naleznete na webu www.legitscript.com.

Předstírání jiné identity a duševní vlastnictví

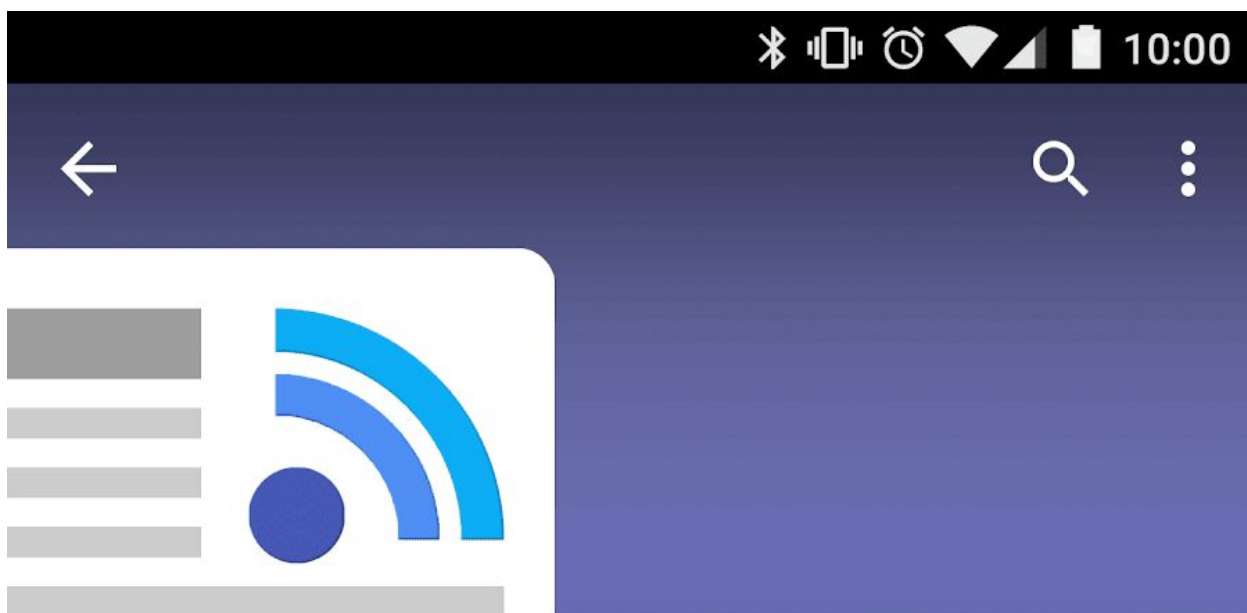
Když vývojáři kopírují cizí práci nebo používají klamavé praktiky, má to špatný vliv na uživatele i na komunitu vývojářů. Nespoléhejte se na zavádějící nebo neférové využívání cizí práce.

Předstírání jiné identity

Nepovolujeme aplikace, které používají značku, název, logo nebo popis jiné aplikace či subjektu způsobem, který by mohl klamat uživatele. Nesnažte se klamavě naznačovat podporu nebo vztah s jiným subjektem. K předstírání jiné identity může dojít i v případě, že uživatele klamat nechcete. Pokud zmiňujete značky, které vám nepatří, buďte opatrní. Platí to i v případě, že se značka zatím na Google Play nevyskytuje.

Aby platforma Google Play zůstala bezpečná a zdvořilá, vytvořili jsme standardy, které definují a zakazují obsah škodlivý nebo nevhodný pro uživatele.

Vývojáři, kteří nepravdivě naznačují vztah s jiným subjektem:



1

RSS News Aggregator

Google Developer

E Everyone

INSTALL



Downloads



161,251 



News &
Magazines



Similar

All the best news, aggregated in one spot!



WHAT'S NEW

- Push notifications now enabled.

- Customize your feed based on your current location!

① Jméno vývojáře uvedené u této aplikace naznačuje oficiální vztah se společností Google, ačkoli žádný takový vztah neexistuje. Názvy a ikony aplikace jsou natolik podobné názvům nebo ikonám existujících produktů či služeb, že to může být pro uživatele zavádějící:

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

Aplikace, které nepravdivě uvádějí, že jsou oficiální aplikací zavedeného subjektu. Bez potřebných oprávnění nebo práv nelze používat například názvy jako Oficiální aplikace Karla Gotta.

Aplikace porušující [pokyny pro použití značky Android](#).

Duševní vlastnictví

Nepovolujeme aplikace ani účty vývojářů, které porušují práva duševního vlastnictví jiných lidí (včetně ochranných známek, autorských práv, patentů, obchodních tajemství a jiných vlastnických práv). Také nepovolujeme aplikace, které k porušování práv duševního vlastnictví vybízejí nebo ho podporují.

Na jasná oznámení o údajném porušení autorských práv budeme reagovat. Další informace naleznete na stránce s našimi [postupy v oblasti autorských práv](#). Na této stránce můžete také podat žádost podle zákona DMCA.

Chcete-li podat stížnost na prodej nebo propagaci prodeje padělaného zboží v aplikaci, odešlete [oznámení o padělení](#).

Pokud jste vlastníkem ochranné známky a domníváte se, že některá z aplikací na Google Play vaše práva k ochranné známce porušuje, doporučujeme obrátit se přímo na jejího vývojáře. Pokud problém s vývojářem nevyřešíte, odešlete stížnost na porušení ochranné známky pomocí tohoto [formuláře](#).

Pokud máte písemné potvrzení, že v aplikaci nebo záznamu v obchodu smíte použít duševní vlastnictví třetí strany (např. název a logo značky, grafické podklady apod.), před odesláním

aplikace [kontaktujte tým podpory Google Play](#), aby bylo zajištěno, že aplikace nebude zamítnuta z důvodu porušení duševního vlastnictví.

Neoprávněné použití obsahu chráněného autorskými právy

Nepovolujeme aplikace porušující autorská práva. K porušení může vést i upravování obsahu chráněného autorskými právy. Pokud vývojář používá obsah chráněný autorskými právy, může být vyzván k předložení důkazu, že je k takovému použití oprávněn.

Buďte opatrní i v případě, že obsah chráněný autorskými právy používáte k předvádění funkcí aplikace. Obecně platí, že nejbezpečnější je vytvářet původní obsah.

Aby platforma Google Play zůstala bezpečná a zdvořilá, vytvořili jsme standardy, které definují a zakazují obsah škodlivý nebo nevhodný pro uživatele.

- Obálka hudebního alba, videohry nebo knihy.

- Marketingové obrázky z filmů, televize nebo videoher.

- Díla nebo obrázky z komiksů, kreslených seriálů, filmů, hudebních videí nebo televize.

- Loga vysokých škol a profesionálních sportovních týmů.

- Fotografie pořízené z účtu veřejně známé osobnosti na sociálních médiích.

- Profesionální snímky veřejně známých osobností.

- Reprodukce nebo „fan art“, které nelze odlišit od původního díla chráněného autorskými právy.

- Aplikace se zvukovou klávesnicí, která přehrává zvukové klipy z obsahu chráněného autorskými právy.

- Úplné reprodukce nebo překlady knih, které se nenacházejí ve veřejném vlastnictví.

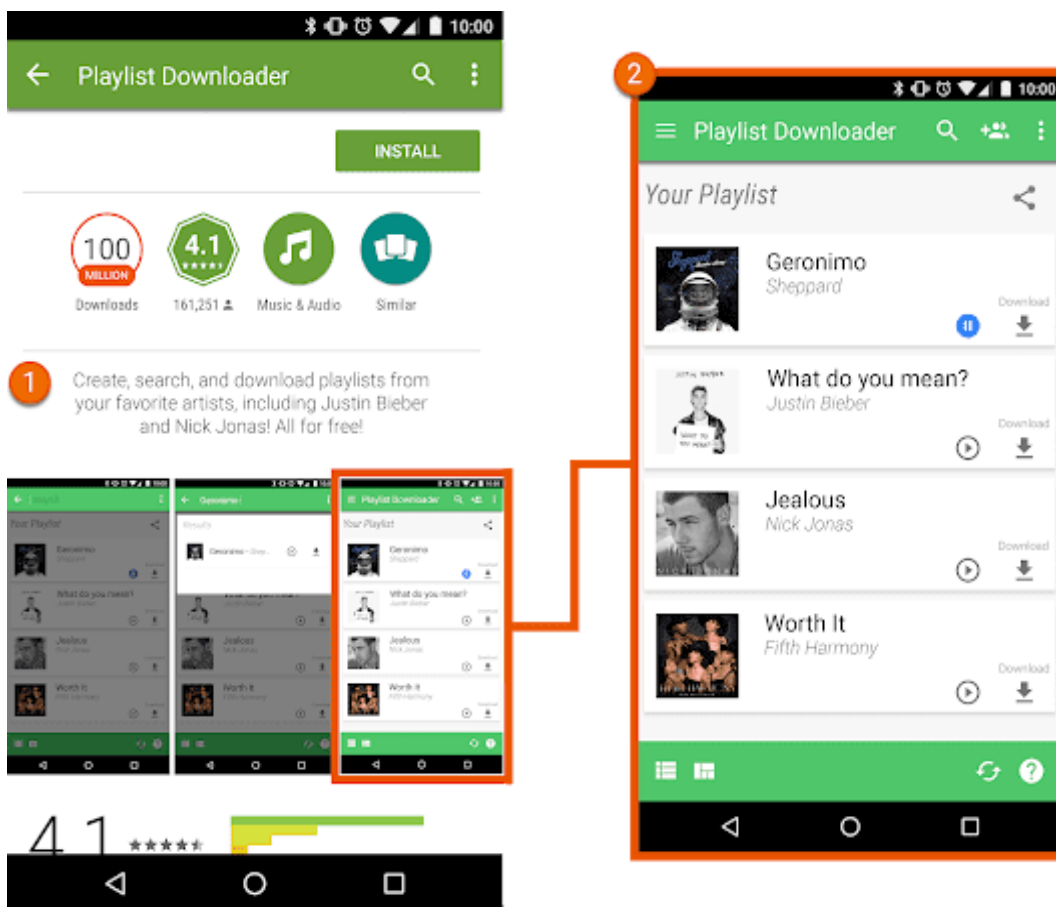
Podpora porušování autorských práv

Nepovolujeme aplikace, které podněcují k porušování autorských práv nebo ho podporují. Před publikováním aplikace se zamyslete nad tím, zda nějakým způsobem nevybízí k porušování autorských práv, a v případě potřeby vyhledejte právní poradenství.

Aby platforma Google Play zůstala bezpečná a zdvořilá, vytvořili jsme standardy, které definují a zakazují obsah škodlivý nebo nevhodný pro uživatele.

- Streamovací aplikace, které uživatelům umožňují stáhnout místní kopii obsahu chráněného autorskými právy bez potřebného povolení.

- Aplikace, které uživatele vybízejí ke streamování a stahování děl chráněných autorskými právy (včetně hudby a videí) způsobem, při kterém dochází k porušení autorských práv:



- ① Popis v tomto záznamu aplikace uživatele vybízí ke stahování obsahu chráněného autorskými právy bez povolení.
- ② Snímek obrazovky v záznamu aplikace uživatele vybízí ke stahování obsahu chráněného autorskými právy bez povolení.

Porušení ochranné známky

Nepovolujeme aplikace, které porušují ochranné známky třetích stran. Ochranná známka je slovo, symbol nebo jejich kombinace, která označuje původ produktu nebo služby. Po přidělení poskytuje ochranná známka svému vlastníkovvi výhradní právo na použití ochranné známky v souvislosti s určitými produkty nebo službami.

Jako porušení ochranné známky se označuje nevhodné nebo nedovolené použití identické nebo podobné ochranné známky (způsobem, který pravděpodobně vyvolá nejistotu ohledně původu daného produktu). Pokud aplikace používá ochrannou známku způsobem, který by mohl vést k nejasnostem, může být pozastavena.

Padělání

Nepovolujeme aplikace, které prodávají nebo propagují prodej padělaného zboží. Padělky jsou opatřeny logem nebo ochrannou známkou, která je identická s jinou ochrannou známkou nebo je od ní téměř neodlišitelná. Snaží se vydávat za originální produkt vlastníka značky tím, že napodobují prvky spojené se značkou daného produktu.

Musíte být transparentní ohledně toho, jak zacházíte s údaji o uživateli (např. s informacemi, které jste o něm a jeho zařízení shromáždili). Uživatele musíte informovat, že aplikace shromažďuje, používá a sdílí data, a smíte data používat jen k účelům, o kterých jste uživatele informovali. Pokud aplikace zpracovává osobní nebo citlivé údaje o uživateli, vztahují se na ni další požadavky (viz sekce Osobní a citlivé údaje níže). Tyto požadavky služby Google Play platí nad rámec povinností, které vyplývají z platných právních předpisů na ochranu soukromí a osobních údajů.

Osobní a citlivé údaje

Mezi osobní a citlivé údaje patří mimo jiné údaje umožňující zjištění totožnosti, finanční a platební údaje, ověřovací údaje, telefonní seznam, kontakty, [poloha zařízení](#), údaje související se zprávami SMS a hovory, data z mikrofonu a fotoaparátu a jiné citlivé údaje o zařízení a jeho využití. Pokud aplikace zpracovává citlivé údaje o uživateli, máte následující povinnosti:

Shromažďování, využívání a sdílení osobních a citlivých údajů získaných prostřednictvím aplikace musíte omezit pouze na účely, které přímo souvisí s poskytováním a vylepšováním funkcí aplikace (např. funkčnost, kterou uživatel očekává a která je zdokumentována a inzerována v popisu aplikace v Obchodě Play). Aplikace, které tyto údaje používají také k zobrazování reklam, musí splňovat naše [zásady inzerce](#).

Uvést zásady ochrany soukromí v označeném poli ve službě Play Console a přímo v aplikaci. Zásady ochrany soukromí společně s případnými oznámeními v aplikaci musí jasně vysvětlovat, jak aplikace získává, shromažďuje, využívá a sdílí údaje o uživatelích. V zásadách ochrany soukromí musí být uvedeno, které typy osobních a citlivých údajů aplikace shromažďuje, používá a sdílí a komu je poskytuje.

Zpracovávat všechny uživatelské údaje zabezpečeným způsobem včetně přenosu šifrovaného moderními metodami (např. pomocí protokolu HTTPS).

Pokud je to možné, používat žádost o oprávnění za běhu před přístupem k údajům pomocí [oprávnění systému Android](#).

Osobní ani citlivé údaje o uživateli nesmíte nikomu prodat.

Požadavky na viditelné oznámení a souhlas

V případech, kdy by uživatelé podle uvážení zástupců služby Play nemuseli přiměřeně očekávat, že k poskytování či vylepšováním funkcí aplikace, které jsou v souladu se zásadami, budou potřeba jejich osobní nebo citlivé údaje, máte následující povinnosti:

Aplikace musí obsahovat oznámení o přístupu k datům, jejich shromažďování, využívání a sdílení. Toto oznámení musí splňovat následující předpoklady:

Musí být přímo v aplikaci, nikoli pouze v popisu aplikace či na webu.
Musí se zobrazovat při běžném používání aplikace a nesmí vyžadovat, aby uživatel přešel do nabídky nebo nastavení.
Musí popisovat, jaká data se používají nebo shromažďují.
Musí vysvětlovat, jakým způsobem budou data využita či sdílena.
Nesmí být umístěno pouze v zásadách ochrany soukromí nebo smluvních podmínkách.
Nesmí být zahrnuto mezi ostatními oznámeními, která se netýkají shromažďování citlivých nebo osobních údajů.

Oznámení v aplikaci se musí zobrazovat těsně před žádostí o souhlas uživatele a, pokud je k dispozici, i před související žádostí o svolení za běhu. Osobní a citlivé údaje smíte začít používat a shromažďovat až poté, co k tomu uživatel udělí souhlas. Žádost aplikace o souhlas musí splňovat následující předpoklady:

Dialogové okno žádosti o souhlas musí být prezentováno jasně a jednoznačně.
K přijetí musí být nutná pozitivní akce uživatele (např. klepnutí na tlačítko, zaškrtnutí políčka).
Opuštění oznámení (např. zavření okna, klepnutí na tlačítko Zpět nebo stisknutí tlačítka plochy) nesmí být považováno za vyjádření souhlasu. .
V žádosti nesmí být použity zprávy, které se samy zavřou (např. po vypršení časového limitu).

Aby platforma Google Play zůstala bezpečná a zdvořilá, vytvořili jsme standardy, které definují a zakazují obsah škodlivý nebo nevhodný pro uživatele.

Aplikace, která informace o nainstalovaných aplikacích uživatele nepovažuje za osobní nebo citlivá data na základě zásad ochrany soukromí, bezpečného přenosu a viditelných oznámení.
Aplikace, která telefonní číslo a seznam kontaktů uživatele nepovažuje za osobní nebo citlivá data na základě zásad ochrany soukromí, bezpečného přenosu a viditelných oznámení.
Aplikace, která zaznamenává obsah obrazovky uživatele a se získaným záznamem nezachází jako s osobními či citlivými daty v souladu s těmito zásadami.
Aplikace používá **polohu zařízení**, aniž by o tom poskytovala úplné informace v souladu s výše uvedenými požadavky.

Omezení přístupu k citlivým údajům

Kromě výše uvedených požadavků platí ještě požadavky pro konkrétní aktivity, které jsou popsány v tabulce níže.

Aktivita	Požadavek
----------	-----------

Aplikace zpracovává identifikační, finanční nebo platební údaje nebo identifikační čísla přidělená státními orgány	Aplikace nesmí nikdy zveřejnit žádné osobní ani citlivé údaje o uživateli související s finančními nebo platebními aktivitami nebo s identifikačními čísly vydanými státními orgány.
Aplikace zpracovává neveřejné telefonní seznamy nebo kontaktní údaje	Není dovoleno bez oprávnění zveřejňovat neveřejné kontakty lidí.
Aplikace obsahuje antivirové, antimalwarové nebo jiné bezpečnostní funkce	Aplikace musí zveřejnit zásady ochrany soukromí, které spolu s případnými oznámeními v aplikaci jasně vysvětlí, jaké uživatelské údaje budou shromažďovány a přenášeny, jak budou využívány a s kým budou sdíleny.

EU-US Privacy Shield

Pokud zobrazujete, používáte nebo zpracováváte osobní údaje zpřístupněné Googlem, které umožňují přímé či nepřímé zjištění totožnosti osoby a které pocházejí ze zemí Evropské unie nebo Švýcarska („osobní údaje z EU“), máte následující povinnosti:

Musíte dodržovat všechny příslušné zákony, směrnice, předpisy a pravidla související s ochranou soukromí, zabezpečením dat a ochranou dat.

Osobní údaje z EU smíte zobrazovat, používat a zpracovávat pouze k účelům, ke kterým vám dal příslušný uživatel souhlas.

Musíte implementovat nezbytné organizační a technické prostředky k ochraně osobních údajů z EU proti ztrátě, zneužití, zveřejnění, pozměnění, zničení a neautorizovanému či nezákonnému přístupu.

Musíte poskytnout stejnou úroveň ochrany, jakou vyžadují [principy programu Privacy Shield](#).

Soulad s těmito podmínkami musíte pravidelně kontrolovat. Pokud tyto podmínky někdy nebudete moci splnit (nebo pokud bude existovat významné riziko, že je nebudete moci splnit), musíte nás o tom ihned informovat zasláním e-mailu na adresu data-protection-office@google.com a buď ihned osobní údaje z EU přestat zpracovávat, nebo podniknout přiměřené kroky k obnovení dostatečné úrovně ochrany.

Žádosti o oprávnění by uživatelům měly dávat smysl. Můžete žádat pouze o oprávnění nezbytná k implementaci existujících funkcí nebo služeb v aplikaci, které inzerujete v záznamu v Obchodu Play. Nesmíte žádat o přístup k údajům o uživateli nebo zařízení za účelem využití v neuvedených, neimplementovaných nebo nedovolených funkcích. Osobní a citlivé údaje získané prostřednictvím oprávnění je zakázáno prodávat.

Snažte se o přístup k údajům žádat co nejvíce v kontextu (prostřednictvím inkrementální autorizace), aby uživatelé věděli, proč dané oprávnění nebo údaje potřebujete. Údaje používejte

pouze k účelům, ke kterým uživatel dal souhlas. Pokud později budete chtít údaje použít k jiným účelům, bude nutné uživatele požádat o výslovné svolení.

Omezená oprávnění

Omezená oprávnění jsou v dokumentaci pro vývojáře označena štítkem **Podpis** nebo **Nebezpečné** a vztahují se na ně následující dodatečné požadavky a omezení:

Citlivé údaje o uživatelích či zařízeních chráněné omezenými oprávněními je dovoleno poskytnout třetím stranám pouze v případě, že je to potřeba k poskytování či vylepšení aktuálních funkcí nebo služeb v aplikaci, z níž příslušná data byla získána. Data můžete převést také v případě, že je to nezbytné ke splnění příslušných právních předpisů, či v rámci sloučení, akvizice nebo prodeje aktiv, přičemž o tom je třeba uživatele právně přiměřeným způsobem informovat. Veškeré jiné převody a prodeje dat uživatelů jsou zakázány.

Pokud uživatel žádost o omezené oprávnění odmítne, respektujte jeho rozhodnutí. Není dovoleno snažit se uživatele zmanipulovat k souhlasu s oprávněními, která nejsou kriticky nutná, ani je k souhlasu s takovými oprávněními nutit. Musíte vyvinout přiměřené úsilí k podpoře uživatelů, kteří přístup k citlivým údajům neposkytnou (např. umožnit ruční zadání telefonního čísla, pokud uživatel odmítne přístup k seznamu hovorů).

Na některá omezená oprávnění se mohou vztahovat další požadavky popsané níže. Cílem těchto omezení je ochránit soukromí uživatelů. Ve velmi ojedinělých případech, kdy aplikace poskytuje velmi zajímavou nebo kriticky důležitou funkci, kterou v současné době nelze poskytovat žádným jiným způsobem, můžeme udělit omezené výjimky z níže uvedených požadavků. Navrhované výjimky posuzujeme s ohledem na možný dopad na ochranu soukromí a bezpečnosti uživatelů.

Oprávnění k přístupu k SMS a seznamu hovorů

Oprávnění k přístupu k SMS a seznamu hovorů jsou považována za osobní a citlivá data o uživateli a vztahují se na ně zásady uvedené v sekci **Osobní a citlivé údaje** a následující omezení:

Omezené oprávnění

Skupina oprávnění Seznam hovorů (např. READ_CALL_LOG, WRITE_CALL_LOG, PROCESS_OUTGOING_CALLS)

Skupina oprávnění SMS (např. READ_SMS, SEND_SMS, WRITE_SMS, RECEIVE_SMS, RECEIVE_WAP_PUSH, RECEIVE_MMS)

Požadavek

Musí být v zařízení aktivně zaregistrován jako výchozí obslužný nástroj typu Telefon nebo Asistence.

Musí být v zařízení aktivně zaregistrován jako výchozí obslužný nástroj typu SMS nebo Asistence.

Aplikace bez funkce výchozího obslužného nástroje typu SMS, Telefon nebo Asistence toto oprávnění v manifestu deklarovat nesmějí. Týká se to i zástupného textu v manifestu. Aplikace také musí být aktivně zaregistrovány jako výchozí obslužné nástroje typu SMS, Telefon nebo Asistent ještě předtím, než uživatele požádají o výše uvedená oprávnění. Jakmile funkci výchozího obslužného nástroje přestanou vykonávat, musí tato oprávnění neprodleně přestat používat. Povolená použití a výjimky jsou k dispozici na [této stránce centra nápovědy](#).

Aplikace mohou oprávnění (a jakákoli data od oprávnění odvozená) používat pouze k poskytování schválené základní funkčnosti aplikace. Může zahrnovat sadu základních funkcí, které musejí být všechny jasně zdokumentovány a propagovány v popisu aplikace. Bez základních funkcí by aplikace byla považována za „rozbitou“ nebo by nebyla použitelná. Přenos, sdílení nebo licencované použití těchto dat je možné pouze za účelem poskytování základních funkcí či služeb v aplikaci a nesmí mít žádný jiný účel (např. vylepšování jiných aplikací či služeb, reklamy nebo marketingové účely). Data, na která se vztahují oprávnění související se seznamem hovorů a zprávami SMS, nesmíte odvozovat alternativními metodami (včetně jiných oprávnění, rozhraní API či externích zdrojů).

Oprávnění pro přístup k poloze

Aktualizace ze 16. dubna 2020: Uvědomujeme si, že splnění zásad ohledně zjišťování polohy může od vývojářů vyžadovat dost práce, proto vám dáváme delší čas, abyste potřebné změny mohli provést. Časový harmonogram a další aktuální informace naleznete v [centru nápovědy](#).

[Poloha zařízení](#) je považována za osobní a citlivý údaj o uživateli a vztahují se na ni zásady uvedené v sekci [Osobní a citlivé údaje](#) a následující omezení:

Data chráněná oprávněními pro přístup k poloze (např. ACCESS_FINE_LOCATION, ACCESS_COARSE_LOCATION, ACCESS_BACKGROUND_LOCATION) mohou aplikace využívat, jen dokud jsou nutná k poskytování aktuálních funkcí nebo služeb v aplikaci. Oprávnění pro přístup k poloze od uživatelů nikdy nesmíte požadovat pouze pro účely inzerce či analýz. Aplikace, které tato data používají také k zobrazování reklam, musí splňovat naše [zásady inzerce](#).

Aplikace musí žádat o nejnižší úroveň přístupu (tj. přibližnou polohu namísto přesné a přístup k poloze na popředí namísto přístupu na pozadí), která je nezbytná k poskytování aktuální funkce nebo služby, a uživatelé by měli přiměřeně očekávat, že funkce nebo služba vyžaduje požadovanou úroveň přístupu k poloze. Můžeme například odmítnout aplikace, které požadují nebo používají přístup k poloze na pozadí bez přesvědčivého zdůvodnění.

Přístup k poloze na pozadí je dovoleno používat pouze k poskytování funkcí, které jsou přínosné pro uživatele a relevantní k hlavní funkci aplikace.

Na získávání údajů o poloze pomocí služby v popředí (když má aplikace povolený pouze přístup na popředí, tj. „během používání“) se vztahují následující podmínky:

Aplikace tyto údaje smí použít pouze jako pokračování akce v aplikaci iniciované uživatelem.

Jakmile aplikace akci iniciovanou uživatelem dokončí, musí údaje o poloze přestat používat.

Aplikace navržené speciálně pro děti musí splňovat zásady programu [Pro celou rodinu](#).

Nepovolujeme aplikace, které neoprávněně zasahují do zařízení uživatele, jiných zařízení či počítačů, sítí, serverů, rozhraní API nebo služeb (mimo jiné včetně jiných aplikací v zařízení, služeb Google nebo sítě autorizovaného operátora), popř. které je narušují, poškozují nebo v nich získávají neoprávněný přístup.

Aplikace na Google Play musejí splnit požadavky na optimalizaci pro výchozí systém Android popsané v [pokynech pro zajištění kvality aplikací na Google Play](#).

Aby platforma Google Play zůstala bezpečná a zdvořilá, vytvořili jsme standardy, které definují a zakazují obsah škodlivý nebo nevhodný pro uživatele.

Aplikace, které blokují nebo narušují zobrazování reklam v jiných aplikacích.

Aplikace pro podvádění ve hrách, které ovlivňují hraní v jiných aplikacích.

Aplikace, které pomáhají napadat služby, software a hardware nebo obcházet bezpečnostní ochranu.

Aplikace, které používají službu nebo rozhraní API způsobem, jenž porušuje smluvní podmínky služby nebo rozhraní.

Aplikace, které se pokoušejí obejít [systémové řízení spotřeby](#) a nesplňují podmínky pro [zařazení na seznam povolených aplikací](#).

Aplikace, které zprostředkovávají služby proxy třetím stranám, tak mohou činit pouze v případech, že se jedná o primární a pro uživatele jasně viditelný účel aplikace.

Nepovolujeme aplikace, které odcizují údaje, tajně sledují uživatele nebo jim škodí, popř. vykazují jiné škodlivé chování.

Aplikace distribuovaná prostřednictvím Google Play nesmí upravovat, nahrazovat ani aktualizovat sebe sama jiným způsobem než pomocí aktualizčních mechanismů služby Google Play. Stejně tak nesmí aplikace stahovat spustitelný kód (např. soubory DEX, JAR, .SO) z jiného zdroje než Google Play. Toto omezení se nevztahuje na kód, který je spuštěn na virtuálním počítači a má omezený přístup k rozhraním Android API (například JavaScript v komponentě WebView nebo prohlížeči).

Dodatečné zdroje aplikací (například herní podklady) je dovoleno stahovat jen v případě, že jsou k používání aplikace nezbytné. Stahované zdroje musejí splňovat všechny zásady služby Google Play a před zahájením stahování by aplikace měla uživatele jasně informovat o velikosti stahovaného obsahu a požádat ho o svolení.

Aplikace na sledování a komerční spyware jsou na Google Play výslovně zakázány. Jediné aplikace s funkcemi sledování a hlášení, které lze na Google Play distribuovat, jsou aplikace navržené a propagované jako nástroje rodičovské kontroly nebo nástroje pro firemní správu. Tyto aplikace musí být v úplném souladu s níže uvedenými požadavky.

Explicitně zakázány jsou:

- viry, trojské koně, malware, spyware nebo jiný škodlivý software,
- aplikace, které odkazují na škodlivý software, popř. zprostředkovávají jeho distribuci nebo instalaci,
- aplikace nebo soubory SDK, které stahují spustitelný kód (například soubory DEX nebo nativní kód) z jiného zdroje než Google Play,
- aplikace, které vytvářejí nebo zneužívají chyby zabezpečení,
- Aplikace, které odcizují ověřovací údaje uživatelů (např. uživatelská jména či hesla) nebo napodobují jiné aplikace nebo weby s cílem oklamat uživatele a přimět je ke zveřejnění osobních nebo ověřovacích údajů.
- aplikace, které zobrazují neověřená nebo reálná telefonní čísla, kontakty, adresy nebo jiné údaje umožňující zjištění totožnosti různých osob nebo subjektů bez jejich souhlasu,
- Aplikace, které instalují do zařízení jiné aplikace bez předchozího souhlasu uživatele.
- aplikace, které stahují obsah ze sítí CDN, aniž by uživatele před zahájením stahování informovaly o velikosti stahovaného obsahu a požádali o svolení,
- aplikace navržené k tajnému shromažďování údajů o využití zařízení (např. komerční spywarové aplikace).

Aplikace, které v zařízení měří nebo sledují chování uživatele, musejí splňovat následující požadavky:

- Aplikace se nesmějí prezentovat jako řešení určené ke špehování nebo skrytému sledování.

- Aplikace nesmějí skrývat ani maskovat sledovací funkce ani o nich uživatele mylně informovat.

- Uživatelům musíte zobrazovat oznámení a jedinečnou ikonu, které aplikaci jasně identifikují.

- Aplikace a zápisy aplikací na Google Play nesmí žádným způsobem umožňovat aktivaci nebo použití funkcí, které porušují tyto podmínky, jako například propojení se soubory APK, které nesplňují zásady, hostovanými mimo Google Play.

- Za to, zda vaše aplikace v cílovém národním prostředí neporušuje zákony, nesete výhradní zodpovědnost vy. Aplikace, které budou v místě vydání označeny za protizákonné, budou odstraněny.

Další informace o nejnovějších bezpečnostních problémech, které byly vývojářům na Google Play nahlášeny, naleznete v [programu pro vylepšení zabezpečení aplikací](#). Podrobnosti o zranitelnostech a jejich odstraňování jsou k dispozici v podobě odkazů na stránky podpory u jednotlivých kampaní.

Nepovolujeme aplikace, které se pokoušejí klamat uživatele nebo napomáhají nepoctivému chování, včetně aplikací, které funkčně nejsou možné. Aplikace musejí ve všech částech metadat poskytovat pravdivá sdělení, popisy a obrázky/video funkcí a musejí fungovat v souladu s přiměřeným očekáváním uživatelů. Aplikace nesmějí napodobovat funkce nebo upozornění operačního systému ani jiných aplikací. Jakékoli změny nastavení zařízení musí být

provedeny s vědomím a souhlasem uživatele a uživatel musí mít možnost tyto změny snadno vrátit zpět.

Zavádějící tvrzení

Nepovolujeme aplikace, které obsahují nepravdivé či zavádějící informace nebo tvrzení (např. v popisu, názvu, na ikoně nebo snímcích obrazovky).

Aby platforma Google Play zůstala bezpečná a zdvořilá, vytvořili jsme standardy, které definují a zakazují obsah škodlivý nebo nevhodný pro uživatele.

- Aplikace, které uvádějí nepravdivé informace nebo nepopisují přesně a jasně své funkce:

 - Aplikace, která dle popisu a snímků obrazovky působí jako závodní hra, ale ve skutečnosti je logickou hrou s obrázkem auta.

 - Aplikace, kterou vývojář označí za antivirový software, ale která ve skutečnosti obsahuje pouze textový návod k odstraňování virů.

Názvy vývojářů nebo aplikací, které neodpovídají aktuálnímu stavu nebo výkonu obsahu ve službě Play. (Příklady: Výběr redakce, Nejstahovanější aplikace, Nejoblíbenější placená aplikace).

Aplikace s lékařským nebo zdravotnickým obsahem, které mohou poskytovat nesprávné informace nebo uživateli potenciálně uškodit.

Aplikace, které tvrdí, že obsahují funkce, jež nelze implementovat.

Aplikace, které jsou zařazené do nesprávných kategorií.

Prokazatelně klamavý obsah, který by mohl ovlivnit volební procesy.

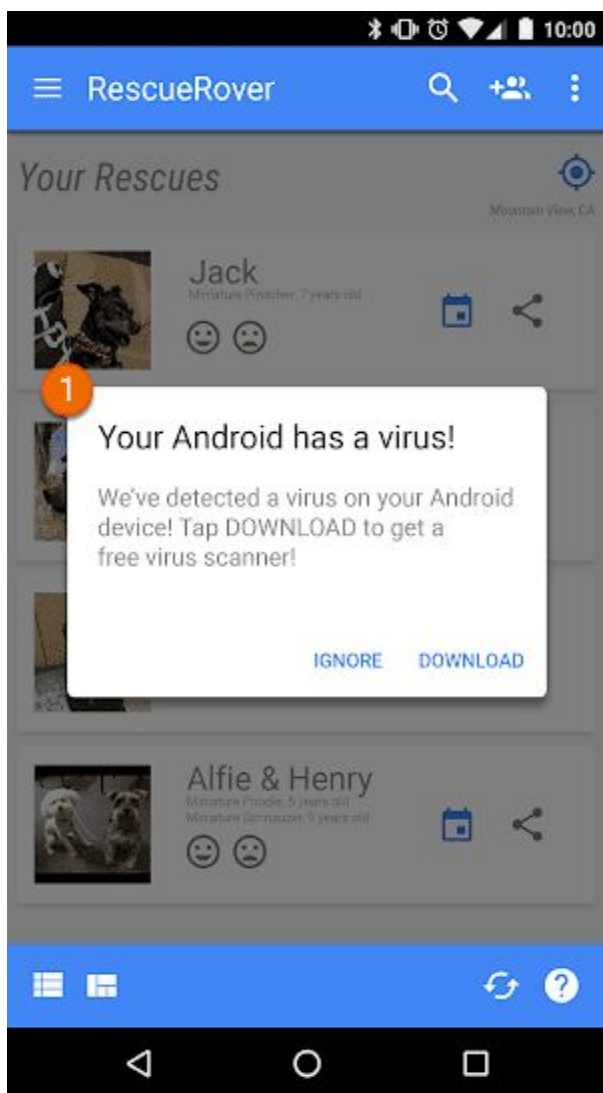
Aplikace, které falešně uvádějí spojení s vládním subjektem nebo zprostředkování služeb státní správy, pro něž nemají oprávnění.

Neoprávněné používání nebo nápodoba funkcí systému

Nepovolujeme aplikace, které napodobují funkce systému (např. oznámení a upozornění) nebo je ovlivňují. Oznámení na úrovni systému lze používat pouze v případě, že se jedná o nedílnou součást funkcí aplikace (například aplikace aerolinek, která uživatele informuje o speciálních nabídkách, nebo hra, která uživatele informuje o propagačních akcích ve hře).

Aby platforma Google Play zůstala bezpečná a zdvořilá, vytvořili jsme standardy, které definují a zakazují obsah škodlivý nebo nevhodný pro uživatele.

- Aplikace nebo reklamy poskytované nebo zobrazované prostřednictvím systémových oznámení nebo upozornění:



① Systémové oznámení objevující se v této aplikaci slouží k zobrazení reklamy.

Další příklady s reklamami naleznete v [zásadách pro reklamy](#).

Klamavé změny nastavení zařízení

Nepovolujeme aplikace, které mění nastavení zařízení uživatele nebo funkce mimo aplikaci, aniž by o tom uživatel věděl nebo s tím souhlasil. Mezi taková nastavení a funkce zařízení patří např. nastavení systému a prohlížeče, záložky, zástupce, ikony, widgety a vizuální prezentace aplikací na ploše.

Kromě výše uvedeného nepovolujeme:

Aplikace, které mění nastavení nebo funkce zařízení se souhlasem uživatele, ale tak, že tyto změny nelze snadno vrátit zpět.

Aplikace nebo reklamy, které mění nastavení nebo funkce zařízení v zájmu třetích stran nebo za účelem inzerce.

Aplikace, které se uživatele snaží oklamat a přimět k odstranění nebo deaktivaci aplikací třetích stran nebo ke změně nastavení nebo funkcí zařízení.

Aplikace, které uživatele podněcují nebo motivují k odstranění nebo deaktivaci aplikací třetích stran nebo ke změně nastavení či funkcí zařízení (výjimku tvoří aplikace, u nichž lze prokázat, že se jedná o bezpečnostní software).

Napomáhání nepoctivému chování

Nepovolujeme aplikace, které uživatelům pomáhají klamat ostatní nebo jsou jakýmkoliv způsobem klamavé, včetně aplikací, které generují nebo umožňují generování identifikačních průkazů, rodných čísel, pasů, diplomů, kreditních karet a řidičských průkazů. Aplikace musejí prostřednictvím sdělení, názvů, popisů a obrázků/videí pravdivě a přesně informovat o svých funkcích a obsahu a musejí fungovat v souladu s přiměřeným očekáváním uživatelů.

Zásady se bez výjimky vztahují i na aplikace, o nichž vývojáři tvrdí, že jsou zamýšleny pouze jako vtip nebo jsou určeny pro zábavní účely.

Manipulace s médii

Nepovolujeme aplikace, které pomocí snímků, videí či textu propagují nebo pomáhají vytvářet nepravdivé nebo zavádějící informace či tvrzení. Jsou zakázány aplikace, které propagují či šíří prokazatelně zavádějící či klamavé snímky, videa či texty a mohou způsobit škodu v souvislosti s citlivou událostí, politickými či společenskými problémy či jinými záležitostmi veřejného zájmu.

Pokud aplikace manipulují s médii či upravují média nad rámec běžných redakčně přijatelných úprav ke zvýšení kvality či srozumitelnosti tak, že by průměrné osobě nemuselo být jasné, že příslušná média byla upravena, musejí o úpravách jasně informovat (například přidáním vodoznaku). V případě veřejného zájmu či jasné satiry či parodie lze udělit výjimky.

Aby platforma Google Play zůstala bezpečná a zdvořilá, vytvořili jsme standardy, které definují a zakazují obsah škodlivý nebo nevhodný pro uživatele.

- aplikace, které přidávají veřejnou osobu na demonstraci během politicky citlivé události,
- aplikace, které ve svém záznamu v obchodě inzerují možnost úpravy médií na ukázce veřejné osoby či média z citlivé události,
- aplikace, které upravují mediální klipy tak, aby vypadaly jako zpravodajské vysílání.

Nepovolujeme aplikace ani účty, které předstírají identitu cizí osoby nebo organizace, případně skrývají či nepravdivě uvádějí svého vlastníka nebo primární účel. Nepovolujeme aplikace ani účty vývojářů, které se zapojují do koordinované činnosti s cílem klamat uživatele. Týká se to mimo jiné aplikací a účtů vývojářů, které nepravdivě uvádějí nebo zatajují zemi původu a které cílí obsah na uživatele v jiné zemi.

Naše zásady ohledně malwaru jsou jednoduché – v ekosystému Android, včetně Obchodu Google Play a zařízení uživatelů, by se nemělo vyskytovat škodlivé chování (tj. malware). Prostřednictvím tohoto základního principu se snažíme poskytovat uživatelům a jejich zařízením Android bezpečný ekosystém.

Malware je každý kód, který by mohl uživatele, jejich data či zařízení vystavit riziku. Mezi malware patří například potenciálně škodlivé aplikace, binární kódy a úpravy aplikačních rámců v kategoriích, jako jsou trojské koně, phishing a spyware, přičemž kategorie neustále aktualizujeme a přidáváme nové.

Existuje celá řada různých typů malwaru, obvykle má však malware některý z následujících cílů:

- poškodit integritu zařízení uživatele,
- získat kontrolu nad zařízením uživatele,
- umožnit dálkově ovládané operace, pomocí nichž útočník k napadenému zařízení bude moci získat přístup nebo ho bude moci jinak využívat,
- odesílat osobní či identifikační údaje mimo zařízení bez adekvátního oznámení a souhlasu,
- šířit z napadeného zařízení spam či příkazy, které budou mít dopad na podobná zařízení či sítě,
- okrást uživatele.

Aplikace, binární kód či úprava aplikačního rámce mohou být potenciálně škodlivé a mohou vykazovat škodlivé chování i neúmyslně. Je to dáno tím, že aplikace, binární kódy a úpravy aplikačních rámců mohou fungovat různě v závislosti na různých proměnných. Chování, které je na jednom zařízení Android škodlivé, nemusí na jiném zařízení Android představovat žádné riziko. Zařízení s nejnovější verzí systému Android například nejsou dotčena škodlivými aplikacemi, které ke škodlivému chování využívají zastaralá rozhraní API. Zařízení, které dosud používá jednu z prvních verzí systému Android, však může být vystaveno riziku. Aplikace, binární kódy a úpravy aplikačních rámců jsou označeny za potenciálně škodlivé aplikace či malware, pokud jasně představují riziko pro některá či všechna zařízení Android a uživatele.

Níže uvedené kategorie malwaru odrážejí naše základní přesvědčení, že by uživatelé měli vědět, jak je jejich zařízení využíváno, a snahu poskytovat bezpečný ekosystém, který umožňuje inovaci a kterému uživatelé mohou důvěřovat.

Další informace najdete na webu [Google Play Protect](#).

Zadní vrátka

Kód, který na zařízení umožňuje provádět nechtěné, potenciálně škodlivé vzdáleně ovládané operace.

Tyto operace mohou zahrnovat chování, jehož automatické spouštění by vedlo k zařazení aplikace, binárního kódu či aplikačního rámce do některé z ostatních kategorií malwaru. Výraz „zadní vrátka“ obecně popisuje způsob provádění potenciálně škodlivých aplikací na zařízení.

Nelze ho proto zařadit do konkrétní kategorie, jako jsou například fakturační podvody či komerční spyware. Některá zadní vrátka tak za určitých okolností služba Google Play Protect může klasifikovat jako chybu zabezpečení.

Fakturační podvod

Kód, který uživatele záměrně oklame za účelem automatického naúčtování platby.

Podvod s fakturací mobilních služeb se rozděluje na podvod s SMS, voláním nebo poplatkem.

Podvod s SMS

Kód, který uživatelům účtuje bez jejich souhlasu platbu za odeslání prémiové SMS, nebo se snaží zamaskovat odesílání SMS pomocí skrytí souhlasů s poskytnutím údajů, případně skrytím SMS zpráv od mobilního operátora, které uživatele upozorňují na platby nebo potvrzují předplatné.

Ačkoli některé typy kódu odesílání SMS vlastně neskrývají, spouští další chování, které odpovídá podvodu s SMS. Mezi příklady patří skrývání částí souhlasu s poskytnutím údajů před uživatelem, zajištění nečitelnosti těchto částí a podmíněčně i zatajení SMS zpráv od mobilního operátora, které uživatele informují o platbách nebo potvrzují předplatné.

Podvod s hovorem

Kód, který uživatelům bez jejich souhlasu účtuje platby za hovory na prémiová čísla.

Podvod s poplatkem

Kód, který uživatele podvodem přiměje k předplacení nebo zakoupení obsahu prostřednictvím faktury za mobilní telefon.

Podvod s poplatkem zahrnuje jakýkoli typ fakturace s výjimkou prémiových SMS a hovorů na prémiová čísla. Mezi příklady patří přímá fakturace přes operátora, bezdrátový přístupový bod (WAP) a převod mobilního kreditu. Nejrozšířenějším typem podvodu s poplatkem je podvod přes WAP. Podvod přes WAP může zahrnovat podvodné přiměnění uživatelů ke kliknutí na tlačítko na tajně načteném, transparentním zobrazení WebView. Po provedení příslušné akce je zahájeno opakované předplatné, přičemž SMS nebo e-mail s potvrzením jsou obvykle odcizeny, aby si uživatelé finanční transakce nevšimli.

Komerční spyware

Kód, který přenáší osobní údaje ze zařízení bez dostatečného informování nebo souhlasu a nezobrazuje trvalé oznámení, že k tomu dochází.

Komerční spywarové aplikace přenášejí data jiné straně, než je poskytovatel potenciálně škodlivé aplikace. Povolené typy těchto aplikací mohou používat rodiče ke sledování dětí.

Pomocí těchto aplikací ale nelze sledovat osobu (například manžela nebo manželku) bez jejího vědomí nebo svolení, pokud během přenosu dat není zobrazeno trvalé oznámení.

Odepření služby (DoS)

Kód, který bez vědomí uživatele provádí útok typu odepření služby (DoS) nebo je součástí distribuovaného útoku DoS proti ostatním systémům a zdrojům.

Může se projevovat například odesíláním vysokého počtu požadavků HTTP za účelem nadměrného zatížení vzdálených serverů.

Nepřátelské stahovací programy

Kód, který není potenciálně škodlivý, ale stahuje jiné potenciálně škodlivé aplikace.

O nepřátelské stahování se může jednat za těchto podmínek:

Existuje důvodné přesvědčení, že kód byl vytvořen za účelem šíření potenciálně škodlivých aplikací a stáhnul nějaké potenciálně škodlivé aplikace nebo obsahuje kód, který by mohl stahovat a instalovat aplikace, nebo
Minimálně 5 % aplikací stažených prostřednictvím kódu jsou potenciálně škodlivé aplikace, přičemž platí minimální hranice 500 zjištěných stažených aplikací (tj. 25 zjištěných stažení potenciálně škodlivé aplikace).

Většina prohlížečů a aplikací ke sdílení souborů není považována za nepřátelský stahovací program, pokud splňuje tyto podmínky:

nespouští stahování bez interakce uživatele a
veškeré stahování potenciálně škodlivých aplikací je iniciováno souhlasem uživatele.

Hrozba pro jiné systémy než Android

Kód, který obsahuje hrozby pro jiné systémy než Android.

Tyto aplikace nemohou poškodit uživatele systému Android ani zařízení Android, ale obsahují komponenty, které mohou být škodlivé pro ostatní platformy.

Phishing

Kód, který předstírá, že pochází z důvěryhodného zdroje, žádá uživatele o poskytnutí ověřovacích či fakturačních údajů a odesílá je třetí straně. Do této kategorie patří také kód, který zachycuje identifikační údaje uživatele během přenosu.

Běžnými cíli phishingových útoků jsou bankovní identifikační údaje, čísla platebních karet a přihlašovací údaje k účtům na sociálních sítích a v hrách.

Zneužití zvýšených oprávnění

Kód, který narušuje integritu systému tím, že prolamuje izolovaný prostor aplikace, získává zvýšená oprávnění či mění nebo znemožňuje přístup k základním bezpečnostním funkcím.

Příklady:

- aplikace, která porušuje model oprávnění systému Android či krade identifikační údaje (například tokeny OAuth) jiných aplikací,
- aplikace, které zneužívají některé funkce k tomu, aby je nebylo možné odinstalovat či zastavit,
- aplikace, která deaktivuje SELinux.

Aplikace ke zvýšení oprávnění, které bez oprávnění uživatele odemykají zařízení, jsou klasifikovány jako rootovací.

Ransomware

Kód, který částečně nebo zcela přebírá kontrolu nad zařízením či daty v zařízení a za opětovné poskytnutí přístupu po uživateli vyžaduje platbu nebo provedení nějakého úkonu.

Ransomware často šifruje data na zařízení a vyžaduje platbu za dešifrování, případně na zařízení využívá administrátorské funkce, aby ho běžný uživatel nemohl odstranit. Příklady:

- zablokování přístupu k zařízení a vyžadování platby za jeho opětovné zpřístupnění,
- zašifrování dat na zařízení a vyžadování platby za jejich dešifrování,
- využívání funkcí správce zásad na zařízení k tomu, aby uživatel aplikaci nemohl odstranit.

Z kategorie ransomwaru může být vyňat kód distribuovaný se zařízením a určený primárně ke správě dotovaných zařízení. Musí však splňovat požadavky týkající se bezpečného uzamčení a správy, adekvátního informování uživatelů a získání souhlasu.

Rootování

Kód, který rootuje zařízení.

Je rozdíl mezi neškodlivým a škodlivým rootovacím kódem. Například neškodlivé rootovací aplikace uživatele předem informují o chystaném rootování zařízení a nespouštějí další potenciálně škodlivé akce, které spadají do ostatních kategorií potenciálně škodlivých aplikací.

Škodlivé rootovací aplikace uživatele o chystaném rootování zařízení neinformují, nebo uživatele o rootování předem informují, ale také spouští další akce, které spadají do ostatních kategorií potenciálně škodlivých aplikací.

Spam

Kód, který kontaktům uživatele odesílá nevyžádané zprávy nebo zařízení používá k šíření spamových e-mailů.

Spyware

Kód, který bez adekvátního sdělení či souhlasu odesílá osobní údaje mimo zařízení.

Za spyware například budou považovány aplikace, které bez oznámení nebo pro uživatele neočekávaným způsobem odesílají některé z následujících informací:

Seznam kontaktů

fotky nebo jiné soubory, které se nacházejí na SD kartě nebo které aplikace nevlastní,
obsah z e-mailové schránky uživatele,

seznam hovorů,

seznam zpráv SMS,

webovou historii nebo záložky z výchozího prohlížeče,

informace z datových adresářů jiných aplikací.

Jako spyware může být klasifikováno také chování, které lze považovat za špehování uživatele. Příkladem může být nahrávání zvuku či hovorů na telefonu nebo odcizování dat aplikací.

Trojský kůň

Kód, který se nezdá být škodlivý (například se tváří jako pouhá hra), ale provádí nežádoucí činnost vůči uživateli.

Tato klasifikace se obvykle používá ve spojení s dalšími kategoriemi potenciálně škodlivých aplikací. Trojský kůň má neškodnou a skrytou škodlivou část. Příkladem může být hra, která na pozadí bez vědomí uživatele odesílá prémiové SMS.

Poznámka ohledně neobvyklých aplikací

Pokud služba Google Play Protect u nových či výjimečných aplikací nemá dostatek informací k tomu, aby je schválila jako bezpečné, může je klasifikovat jako neobvyklé. Nemusí to nutně znamenat, že je aplikace škodlivá. Bez další kontroly ji však nelze schválit ani jako bezpečnou.

Poznámka ke kategorii Zpětná vrátka

Do kategorie zpětných vrátek se malware zařazuje podle způsobu chování kódu. Za zpětná vrátka považujeme pouze kód, který umožňuje provádět činnosti, jejichž automatické provádění by vedlo k zařazení kódu do některé jiné kategorie malwaru. Pokud například aplikace umožňuje dynamické načítání kódu a dynamicky načítaný kód extrahuje textové zprávy, bude daná aplikace klasifikována jako malware poskytující zadní vrátka.

Pokud však aplikace umožňuje spouštění libovolného kódu, ale nemáme důvod domnívat se, že tato možnost byla přidána s cílem provádět škodlivé činnosti, budeme to považovat pouze za chybu zabezpečení (nikoliv za malware poskytující zpětná vrátka) a požádáme vývojáře o opravu.

Nepovolujeme aplikace, které obsahují klamavé nebo rušivé reklamy. Reklamy se mohou zobrazovat pouze v aplikaci, která jejich zobrazení realizuje. Reklamy zobrazované v aplikaci považujeme za součást aplikace. Musejí být v souladu se všemi našimi zásadami. Zásady ohledně reklam na hazardní hry naleznete [zde](#).

Google Play podporuje celou řadu strategií zpeněžení, které přinášejí výhody vývojářům i uživatelům. Patří mezi ně například placená distribuce, produkty v aplikacích, předplatné a příjmové modely založené na reklamách. Protože chceme zajistit co nejlepší uživatelský dojem, vyžadujeme, abyste dodržovali následující zásady.

Platby

Aplikace, které používají nákupy v obchodě nebo v aplikaci, se musejí řídit následujícími pokyny:

Nákupy v aplikacích: Vývojáři, kteří účtují poplatky za aplikace a obsah stahovaný z Google Play musí používat platební systém Google Play.

Nákupy v aplikacích:

Vývojáři, kteří nabízejí produkty ve hře stažené z Google Play nebo poskytují přístup k hernímu obsahu, musí jako platební metodu používat [Fakturaci v aplikaci Google Play](#). Vývojáři, kteří nabízejí produkty v jiné kategorii aplikace stažené z Google Play, musí jako platební metodu používat [Fakturaci v aplikaci Google Play](#), kromě následujících výjimek:

Platba slouží výhradně k úhradě fyzických produktů.

Platbou se hradí digitální obsah, který lze využít i mimo samotnou aplikaci (např. skladby, které lze přehrávat i v jiných hudebních přehrávačích).

Virtuální měny v aplikacích smí být používány pouze v aplikaci nebo hře, ve které byly koupeny.

Vývojáři nesmějí uživatele o prodávaných aplikacích informovat zavádějícím způsobem.

Platí to i pro služby, zboží, obsah a funkce prodávané v aplikacích. Pokud v popisu produktu na Google Play informujete o funkcích v aplikaci, které mohou být nějakým dalším způsobem zpoplatněny, musí být z popisu uživatelům jasně patrné, že je přístup k těmto funkcím podmíněn platbou.

Aplikace, které umožňují nákupy náhodných virtuálních položek (tzv. lootboxy), musejí před nákupem jasně informovat o pravděpodobnosti získání takových položek.

Odběry

Jako vývojář nesmíte uživatele klamat ohledně předplacených služeb či obsahu, který v aplikaci nabízíte. Informace v promo textech v aplikaci či na úvodních obrazovkách musí být jasné.

V aplikaci: Nabídka musí být transparentní. Je třeba explicitně uvést podmínky nabídky, cenu předplatného, frekvenci fakturačního cyklu a skutečnost, zda je používání aplikace podmíněno

předplatným. Tyto informace se musí zobrazit automaticky, aniž by uživatel prováděl jakoukoli další akci.

Aby platforma Google Play zůstala bezpečná a zdvořilá, vytvořili jsme standardy, které definují a zakazují obsah škodlivý nebo nevhodný pro uživatele.

Měsíční předplatné uživatele neinformuje o tom, že se bude každý měsíc automaticky obnovovat a strhávat platba.

Roční předplatné nejvýrazněji zobrazují cenu přepočtenou na měsíce.

Cena a podmínky předplatného nejsou náležitě lokalizované (přeložené).

Promo akce v aplikaci, které jasně neuvádějí, že uživatel může získat přístup k obsahu bez předplatného (pokud je tato možnost k dispozici).

Název SKU neodpovídá povaze předplatného (předplatné se například nazývá „Bezplatná zkušební verze“, ačkoliv jsou za něj automaticky účtovány pravidelné platby).

The screenshot shows a subscription offer for 'AnalyzeAPP Premium'. It features a circular illustration of a person at a computer with charts. Below the illustration, it says '16 issues found in your data!' and 'Subscribe to see how we can help'. There are three pricing options: 12 months (\$9.16/mo, Save 35%), 6 months (\$12.50/mo, Save 11%, Most Popular Plan), and 1 month (\$14.00/mo). A blue button says 'Try for \$12.50!'. At the bottom, there is a cancellation notice in Spanish.

1 Get AnalyzeAPP Premium

2 12 months
\$9.16/mo
Save 35%

6 months
\$12.50/mo
Save 11%
MOST POPULAR PLAN

1 month
\$14.00/mo

3 Try for \$12.50!

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

- ① Není zobrazeno tlačítko k odmítnutí a uživatelům nemusí být jasné, že funkce mohou používat i bez přijetí nabídky předplatného.
- ② Jsou uvedeny pouze ceny za měsíc a uživatelům nemusí být jasné, že jim při přihlášení k odběru bude naúčtována cena za šest měsíců.
- ③ V nabídce je uvedena pouze zaváděcí cena a uživatelům nemusí být jasné, jaká cena jim bude automaticky naúčtována na konci zaváděcího období.
- ④ Nabídka by měla být lokalizována do stejného jazyka jako smluvní podmínky, aby uživatelé rozuměli celé nabídce.

Bezplatná zkušební období a zaváděcí nabídky

Než si uživatel zaregistruje předplatné: Musíte přesně a srozumitelně popsat podmínky nabídky, včetně délky, ceny a popisu přístupného obsahu nebo služeb. Informujte uživatele, jak a kdy se bezplatné zkušební období změní na placené předplatné, kolik bude placené předplatné stát a že službu bude moci zrušit, pokud na placené předplatné nebude chtít přejít.

Aby platforma Google Play zůstala bezpečná a zdvořilá, vytvořili jsme standardy, které definují a zakazují obsah škodlivý nebo nevhodný pro uživatele.

Nabídky, které jasně nevysvětlují, jak dlouho bude bezplatné zkušební období nebo zaváděcí cena trvat.

Nabídky, které jasně nevysvětlují, že uživatel bude na konci období nabídky automaticky zaregistrován do placeného předplatného.

Nabídky, které jasně neuvádějí, že uživatel může získat přístup k obsahu bez zkušební verze (pokud je tato možnost k dispozici).

Cena a podmínky nabídky nejsou náležitě lokalizované.



- ① Není zobrazeno tlačítko k odmítnutí a uživatelům nemusí být jasné, že funkce mohou používat i bez registrace k bezplatnému zkušebnímu období.
- ② Nabídka zdůrazňuje bezplatné zkušební období a uživatelům nemusí být jasné, že jim na jeho konci bude automaticky naúčtováno předplatné.
- ③ V nabídce není uvedeno, že se jedná o zkušební období. Uživatelům nemusí být jasné, jak dlouho budou mít zdarma přístup k obsahu, který je běžně dostupný pouze předplatitelům.
- ④ Nabídka by měla být lokalizována do stejného jazyka jako smluvní podmínky, aby uživatelé rozuměli celé nabídce.

Správa a rušení předplatných

Jako vývojář musíte zajistit, že v aplikaci bude srozumitelně uvedeno, jak může uživatel předplatné spravovat či zrušit.

Pokud uživatel zruší odběr zakoupený v aplikaci na Google Play, podle našich zásad takovému uživateli nebude vrácena platba za aktuální fakturační období, ale bez ohledu na datum zrušení bude po zbytek aktuálního fakturačního období i nadále dostávat odebíraný obsah. Odběr bude zrušen po skončení aktuálního fakturačního období.

Poskytovatel obsahu nebo přístupu může uživatelům poskytnout flexibilnější pravidla pro vracení peněz. Je vaší odpovědností informovat uživatele o změnách zásad předplatného, rušení předplatných a vracení peněz a zajistit, aby byly tyto zásady v souladu s příslušnými právními předpisy.

Nepovolujeme aplikace, které obsahují klamavé nebo rušivé reklamy. Reklamy se mohou zobrazovat pouze v aplikaci, která jejich zobrazení realizuje. Reklamy zobrazované v aplikaci považujeme za součást aplikace. Musejí být v souladu se všemi našimi zásadami. Zásady ohledně reklam na hazardní hry naleznete [zde](#).

Nepovolujeme aplikace, které obsahují klamavé nebo rušivé reklamy. Reklamy se mohou zobrazovat pouze v aplikaci, která jejich zobrazení realizuje. Reklamy zobrazované v aplikaci považujeme za součást aplikace. Musejí být v souladu se všemi našimi zásadami. Zásady ohledně reklam na hazardní hry naleznete [zde](#).

Používání údajů o poloze pro reklamy

Aplikace, které údaje o poloze zařízení chráněné oprávněním používají k zobrazování reklam, podléhají zásadám uvedeným v sekci [Osobní a citlivé údaje](#) a musejí také splňovat následující požadavky:

O používání nebo shromažďování údajů o poloze zařízení chráněných oprávněním k inzertním účelům musí být uživatel informován a musí být zdokumentováno v povinných zásadách ochrany soukromí aplikace, a to včetně odkazu na zásady ochrany soukromí reklamní sítě, které se týkají používání údajů o poloze.

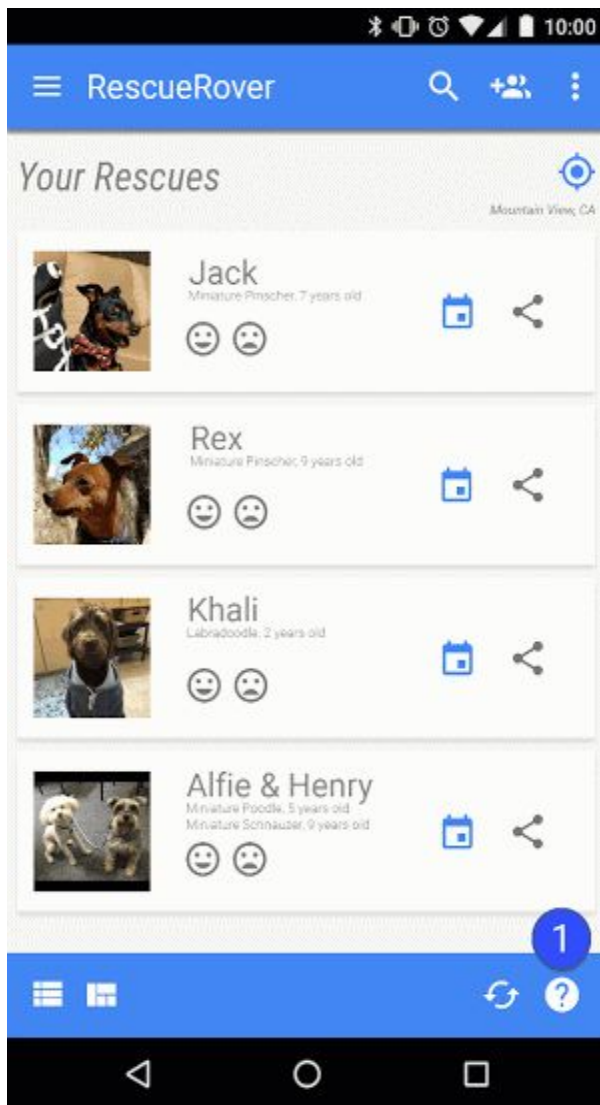
V souladu s požadavky na [oprávnění pro přístup k poloze](#) je o toto oprávnění dovoleno žádat pouze za účelem implementace aktuálních funkcí nebo služeb aplikace. O toto oprávnění není dovoleno žádat výhradně pro účely zobrazování reklam.

Klamavé reklamy

Reklamy nesmějí napodobovat ani se vydávat za uživatelské rozhraní žádné aplikace ani za oznámení či upozornění operačního systému. Uživatelé musí být jasné, ke které aplikaci reklama patří.

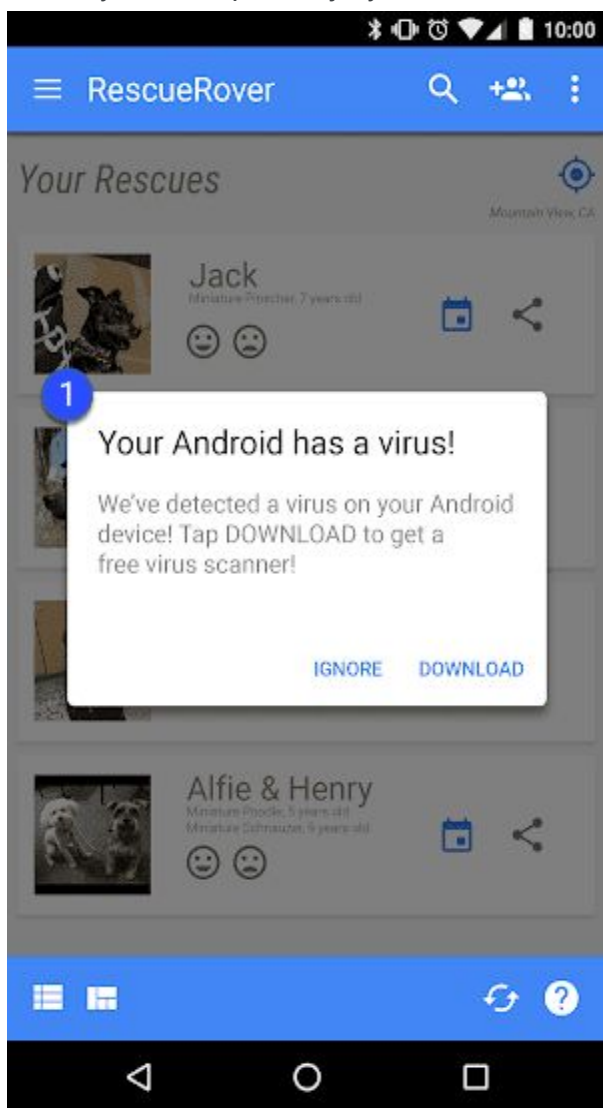
Aby platforma Google Play zůstala bezpečná a zdvořilá, vytvořili jsme standardy, které definují a zakazují obsah škodlivý nebo nevhodný pro uživatele.

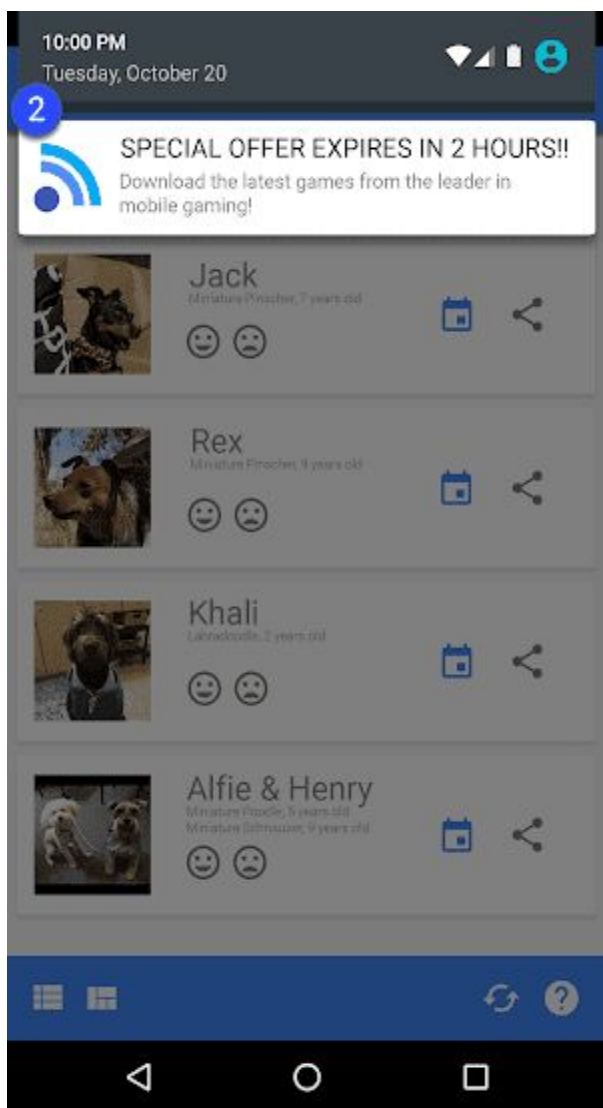
Reklamy, které napodobují uživatelské rozhraní aplikace:



① Ikona otazníku v této aplikaci je reklama, která uživatele přesměrovává na externí vstupní stránku.

Reklamy, které napodobují systémová oznámení:





① ② Výše uvedené příklady znázorňují reklamy napodobující různá systémová oznámení.

Zpeněžení obrazovky uzamčení

Pokud výhradním účelem aplikace není obrazovka uzamčení, nesmí aplikace zahrnovat reklamy ani funkce, které zpeněžují uzamčený displej zařízení.

Rušivé reklamy

Reklamy se nesmějí zobrazovat způsobem, který vede k neúmyslným kliknutím. Podmiňovat používání aplikace v plném rozsahu kliknutím na reklamy nebo odesláním osobních údajů k reklamním účelům je zakázáno.

Vsunuté reklamy se mohou zobrazovat pouze v aplikaci, která jejich zobrazení realizuje. Pokud aplikace zobrazuje vsunuté reklamy nebo jiné reklamy, které narušují běžnou práci s aplikací, musíte uživateli umožnit tyto reklamy snadno zavřít bez jakékoli penalizace.

Aby platforma Google Play zůstala bezpečná a zdvořilá, vytvořili jsme standardy, které definují a zakazují obsah škodlivý nebo nevhodný pro uživatele.

Reklama, která zabere celou obrazovku nebo jinak brání běžné práci s aplikací a neposkytuje jasně viditelnou možnost reklamu zavřít:



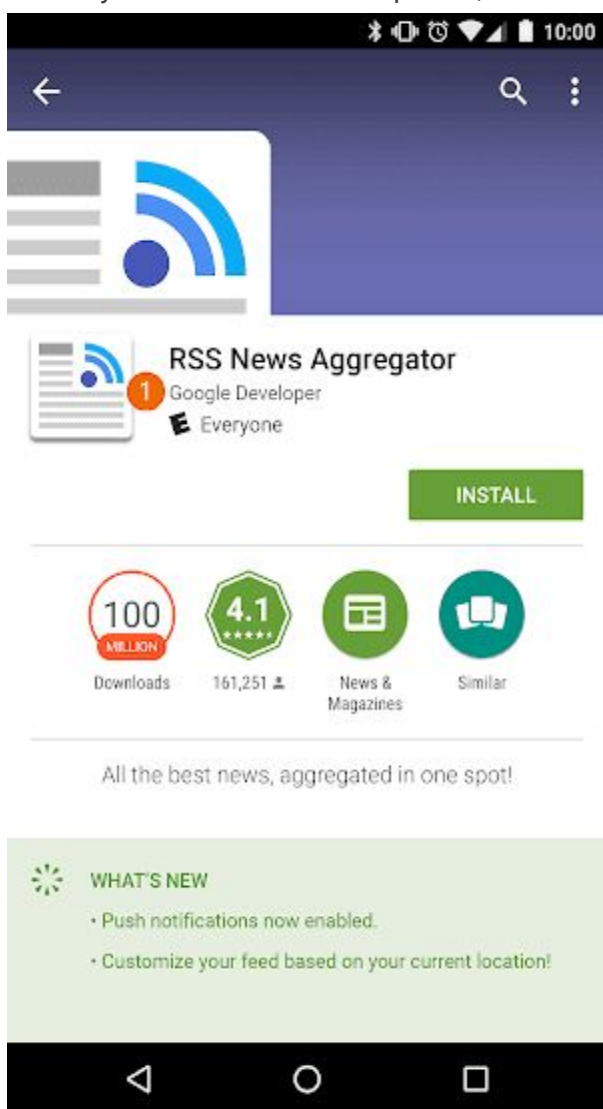
① Tato reklama nemá tlačítko pro zavření.

Zasahování do aplikací, reklam třetích stran nebo funkcí zařízení

Reklamy přidružené k vaší aplikaci nesmějí zasahovat do ostatních aplikací, jejich reklam ani funkcí zařízení (včetně systému a tlačítek nebo portů zařízení). To zahrnuje překryvné reklamy, funkce doprovodné reklamy i reklamní jednotky v podobě widgetů. Reklamy se mohou zobrazovat pouze v aplikaci, která jejich zobrazení realizuje.

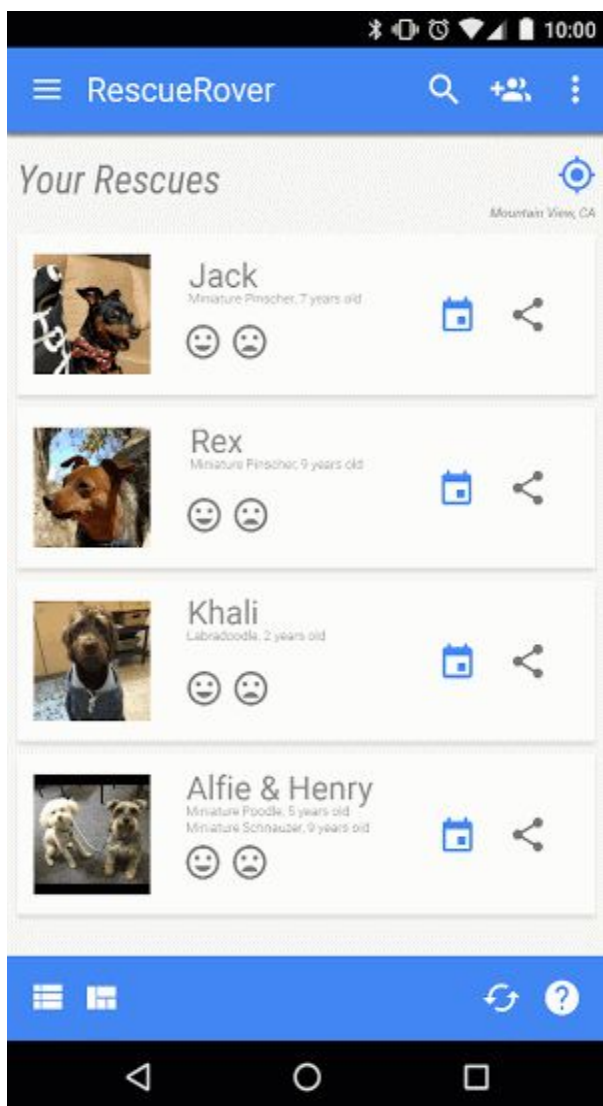
Aby platforma Google Play zůstala bezpečná a zdvořilá, vytvořili jsme standardy, které definují a zakazují obsah škodlivý nebo nevhodný pro uživatele.

Reklamy zobrazované mimo aplikaci, která zobrazení realizuje:



Popis: Uživatel přejde z aplikace na plochu a zničehonic se na ploše zobrazí reklama.

Reklamy spouštěné tlačítkem plochy nebo jinými prvky navrženými k opuštění nebo ukončení aplikace:

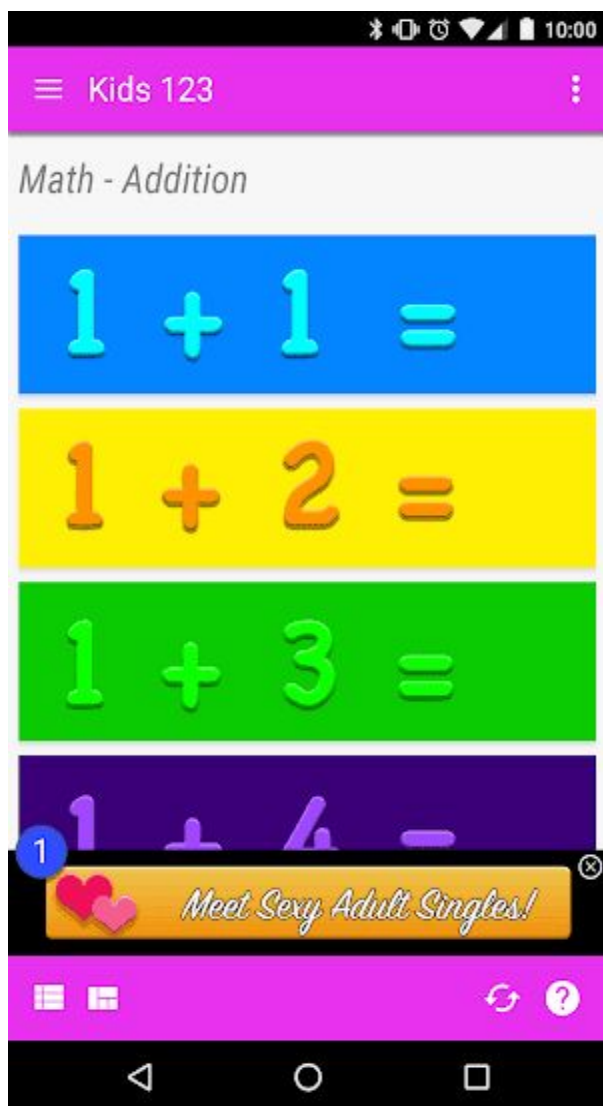


Popis: Uživatel se snaží aplikaci opustit a přejít na plochu, ale očekávaný průběh této operace je narušen reklamou.

Nevhodné reklamy

Reklamy zobrazované v aplikaci musí být vhodné pro cílové publikum aplikace (a to i v případě, že obsah sám o sobě je jinak v souladu s našimi zásadami).

Aby platforma Google Play zůstala bezpečná a zdvořilá, vytvořili jsme standardy, které definují a zakazují obsah škodlivý nebo nevhodný pro uživatele.



① Tato reklama není vhodná pro cílové publikum této aplikace.

Použití inzerčního ID Android

Ve Službách Google Play verze 4.0 byla zavedena nová rozhraní API a identifikátor pro poskytovatele reklamy a analýz. Podmínky využití tohoto identifikátoru jsou uvedeny níže.

Využití. Inzerční identifikátor Android je dovoleno používat pouze pro inzerci a analýzu uživatelů. Při každém přístupu k tomuto identifikátoru musí být zkontrolováno nastavení odhlášení ze zájmově orientované inzerce nebo odhlášení z personalizace reklam. Přidružení k informacím, které umožňují zjištění totožnosti, nebo jiným identifikátorům. Inzerční identifikátor nesmí být bez výslovného souhlasu uživatele přidružen k informacím, které umožňují zjištění totožnosti, ani k žádnému trvalému identifikátoru zařízení (jako jsou například SSAID, MAC adresa, číslo IMEI apod.). Respektování voleb uživatelů. Po resetování nesmí být nový inzerční identifikátor bez výslovného souhlasu uživatele přidružen k předchozímu inzerčnímu identifikátoru ani k

datům z něj odvozeným. Kromě toho musíte respektovat nastavení odhlášení ze zájmově orientované inzerce nebo odhlášení z personalizace reklam daného uživatele. Pokud uživatel toto nastavení aktivoval, nesmíte reklamní identifikátor použít k vytváření profilů uživatelů pro reklamní účely ani k cílení personalizovaných reklam. Mezi povolené aktivity patří zobrazování kontextové inzerce, omezení frekvence, měření konverzí, vytváření přehledů, zabezpečení a zjišťování podvodů.

Transparentnost pro uživatele. Uživatelé musejí být o shromažďování a využití reklamního identifikátoru a závazku dodržovat tyto smluvní podmínky informováni v právně přiměřeném oznámení o ochraně soukromí. Další informace o standardech ochrany soukromí naleznete v článku o zásadách týkajících se [údajů o uživateli](#).

Dodržování smluvních podmínek. Reklamní identifikátor je dovoleno používat pouze v souladu s těmito smluvními podmínkami. Tyto smluvní podmínky musejí dodržovat všechny strany, se kterými reklamní identifikátor v rámci své činnosti sdílíte. Všechny aktualizace a nové aplikace nahrané na Google Play musí namísto jakýchkoliv jiných identifikátorů zařízení pro veškeré reklamní účely používat pouze inzertní ID (pokud je v zařízení k dispozici).

Pokud v aplikaci zobrazujete reklamy a cílovým publikem jsou pouze děti (jak je popsáno v [zásadách pro rodiny](#)), musíte použít reklamní sady SDK, které mají vlastní certifikaci pro Google Play a splňují níže uvedené certifikační požadavky pro reklamní sady SDK. Pokud vaše aplikace cílí na děti i starší uživatele, musíte implementovat opatření na filtrování podle věku uživatelů a zajistit, aby reklamy zobrazované dětem pocházely výhradně z některé z těchto reklamních sad SDK s vlastní certifikací. Aplikace v programu Pro celou rodinu mohou používat pouze reklamní sady SDK s vlastní certifikací.

Použití reklamních sad SDK certifikovaných pro Google Play je povinné pouze v případě, že pomocí nich zobrazujete reklamy dětem. Následující možnosti jsou povoleny bez vlastní certifikace reklamní sady SDK u Google Play, avšak nadále nesete odpovědnost za to, že reklamní obsah a postupy shromažďování údajů budou v souladu se [zásadami pro uživatelská data](#) a [zásadami pro rodiny](#) služby Play:

Vlastní inzerce, při které vydavatelé aplikací používají sady SDK k propagaci svých vlastních aplikací, médií či reklamního zboží

Přímé dohody s inzerenty s využitím sad SDK pro správu inventáře

Požadavky na certifikaci reklamních sad SDK

Definujte nevhodný obsah a chování reklam a ve smluvních podmínkách a zásadách reklamní sady SDK je zakažte. Definice by neměly vést k nesouladu s programovými zásadami služby Play pro vývojáře.

Vytvořte metodu k hodnocení kreativ podle věkových skupin (zahrňte alespoň skupiny Všichni a Pro dospělé). Metodika hodnocení musí odpovídat metodice, kterou certifikovaným sadám SDK po vyplnění formuláře k projevení zájmu poskytuje společnost Google.

Umožněte majitelům obsahu, aby u jednotlivých žádostí nebo jednotlivých aplikací při zobrazování reklam mohli žádat o obsah určený dětem. Zajistit, aby aplikace (včetně všech rozhraní API, sad SDK a reklam) byla v souladu se všemi příslušnými zákony a předpisy ohledně dětí, jako je zákon USA o ochraně soukromí dětí na internetu ([COPPA](#)) nebo obecné nařízení EU o ochraně osobních údajů ([GDPR](#)). Google Play dále vyžaduje, aby u obsahu určeného dětem byly deaktivovány personalizované reklamy, zájmově orientované reklamy a remarketing.

Zajistěte, že pokud budou k zobrazování reklam dětem použity nabídky v reálném čase, kreativy budou zkontrolovány a do systémů generujících nabídky budou předány indikátory ochrany soukromí.

Poskytněte společnosti Google dostatek informací k ověření, zda reklamní sada SDK splňuje všechny certifikační požadavky, a včas odpovídejte na všechny následné žádosti o informace.

Poznámka: Reklamní sady SDK musejí podporovat zobrazování reklam, které je v souladu se všemi relevantními předpisy a nařízeními ohledně dětí, jež se na majitele obsahu mohou vztahovat.

Požadavky na zprostředkování pro reklamní platformy při zobrazování reklam dětem:

Používejte pouze reklamní sady SDK certifikované službou Play nebo implementujte bezpečnostní opatření, která zajistí splnění těchto požadavků u všech reklam zobrazovaných prostřednictvím zprostředkování.

Předávejte signály nutné k určení hodnocení obsahu reklamy a případného obsahu určeného dětem.

Vývojáři si mohou projít [seznam certifikovaných reklamních sad SDK](#).

Poskytovatele reklamních sad SDK, kteří chtějí získat certifikaci, mohou vývojáři také odkázat na tento [formulář k projevení zájmu](#).

Záznamy v obchodu a propagace

Propagace a viditelnost aplikace má velký vliv na kvalitu obchodu. Nepoužívejte spamové záznamy v obchodu, nekvalitní propagaci ani metody pro umělé zvýšení viditelnosti aplikace na Google Play.

Propagace aplikací

Nepovolujeme aplikace, které přímo nebo nepřímo těží z propagačních praktik, jež klamou nebo škodí uživatelům či vývojářskému ekosystému. Jedná se například o aplikace s následujícím chováním:

Používání klamavých reklam na webech, v aplikacích nebo jiných službách, včetně oznámení, která připomínají systémová oznámení či upozornění.

Propagační nebo instalační taktiky, které uživatele přesměrovávají na Google Play nebo spouštějí stahování aplikací bez vědomé akce uživatele.

Nevyžádaná propagace prostřednictvím zpráv SMS.

Je vaší povinností zajistit, aby reklamní sítě nebo spřízněné subjekty přidružené k aplikaci tyto zásady dodržovaly a nepoužívaly žádné zakázané propagační praktiky.

Metadata

Nepovolujeme aplikace s matoucími, nesprávně naformátovanými, irelevantními, nadbytečnými nebo nevhodnými metadaty, včetně popisu aplikace, jména vývojáře, názvu, ikony, snímků obrazovky a propagačních obrázků. Vývojáři musí poskytnout srozumitelný a kvalitně napsaný popis. V popisu aplikace je také zakázáno uvádět anonymní nebo nepřirazená prohlášení uživatelů.

Aby platforma Google Play zůstala bezpečná a zdvořilá, vytvořili jsme standardy, které definují a zakazují obsah škodlivý nebo nevhodný pro uživatele.



- ① Anonymní nebo nepřřazená prohlášení uživatelů
- ② Porovnání dat aplikací nebo značek
- ③ Bloky slov nebo vertikální či horizontální seznamy slov

Zde je několik příkladů nevhodného textu, obrázků a videí v záznamu:

Obrázky nebo videa se sexuálním podtextem. Nepoužívejte reálné ani ilustrované obrázky se sexuálním podtextem, které vyobrazují ňadra, hýždě, genitálie ani jiné části těla či obsah, který může být předmětem sexuálního vzrušení.

Vyjadřování nevhodné pro obecné publikum. V záznamu aplikace nepoužívejte vulgární výrazy. Pokud se jedná o zásadní prvek aplikace, v záznamu v obchodu musí být cenzurován.

Explicitní násilí nápadně vyobrazené v ikonách aplikace, propagačních obrázcích či videích.

Vyobrazení nezákonné konzumace drog. Také obsah vzdělávacího, dokumentárního, vědeckého nebo uměleckého charakteru v záznamu v obchodu musí být vhodný pro všechny kategorie publika.

Zde je několik doporučených postupů:

Zdůrazněte, co je na vaší aplikaci skvělého. Podělte se s uživateli o zajímavá a poutavá fakta, abyste jim pomohli aplikaci odlišit od konkurence.

Název a popis aplikace musí přesně popisovat její funkce.

Nepoužívejte opakující se ani nesouvisející klíčová slova a reference.

Popis aplikace by měl být stručný a výstižný. Kratší popisy bývají pro uživatele lepší, zejména v zařízeních s menším displejem. Příliš dlouhé, podrobné, nesprávně naformátované nebo opakované popisy mohou být považovány za porušení této zásady.

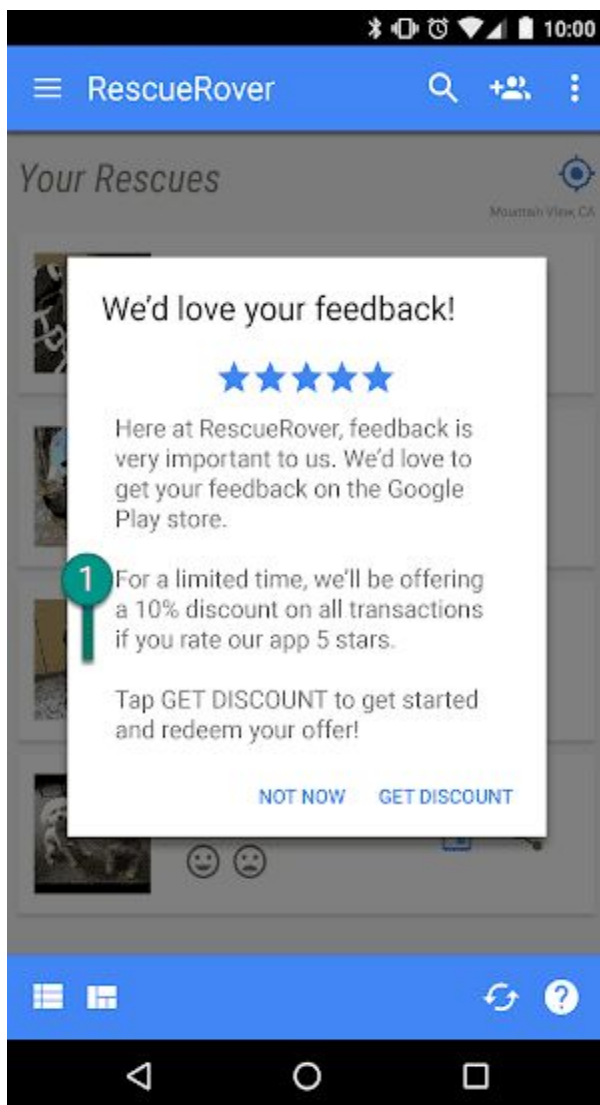
Připomínáme, že záznam musí být vhodný pro obecné publikum. V záznamu nepoužívejte nevhodný text, obrázky ani videa a řiďte se výše uvedenými pokyny.

Uživatelská hodnocení, recenze a instalace

Vývojáři se umístění aplikací na Google Play nesmějí pokoušet zmanipulovat. Mimo jiné je zakázáno například uměle zvyšovat hodnocení produktů nebo počty instalací či recenzí nepovolenými způsoby, jako jsou podvodné nebo pobídkami získané instalace, recenze a hodnocení.

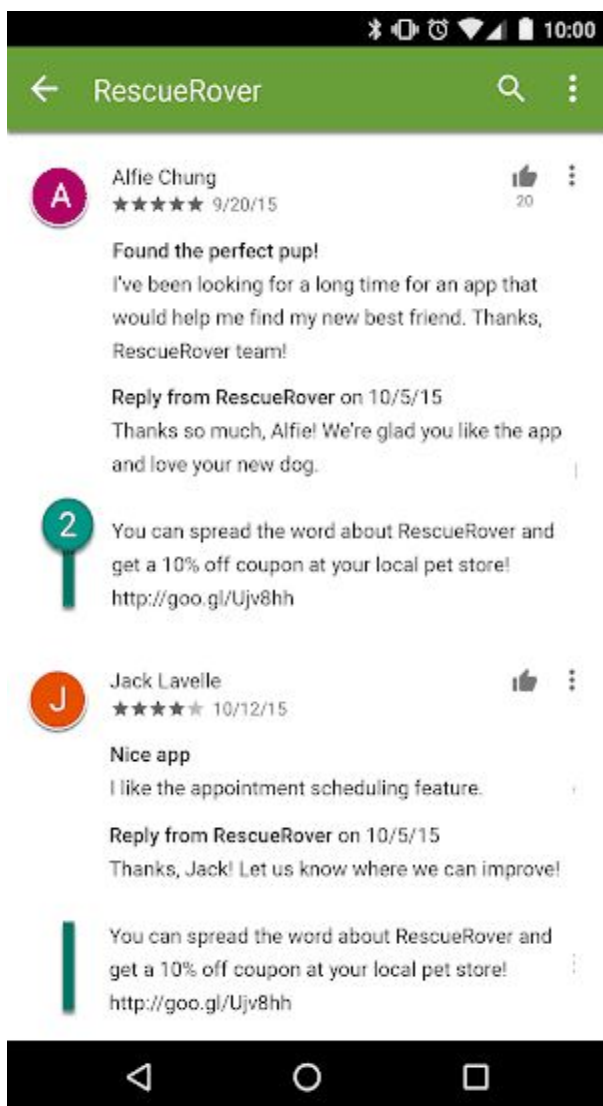
Aby platforma Google Play zůstala bezpečná a zdvořilá, vytvořili jsme standardy, které definují a zakazují obsah škodlivý nebo nevhodný pro uživatele.

Nabízení odměn za hodnocení aplikace:



① Toto oznámení nabízí uživatelům slevu výměnou za vysoké hodnocení aplikace.

Opakované odesílání hodnocení za účelem ovlivnění umístění aplikace na Google Play. Je zakázáno odesílat recenze s nevhodným obsahem (např. s odkazy na partnery, kupóny, herními kódy, e-mailovými adresami nebo odkazy na weby či jiné aplikace) nebo k takovému jednání vybízet uživatele:



② Tato recenze prostřednictvím nabídky kupónu vybízí uživatele k tomu, aby propagovali aplikaci RescueRover.

Hodnocení a recenze slouží jako ukazatele kvality aplikace. Uživatelé se spoléhají, že budou spolehlivé a relevantní. Zde je několik doporučených postupů pro odpovídání na uživatelské recenze:

Odpovědi by se měly soustředit na problémy vznesené v komentářích uživatelů a neměly by žádat o vyšší hodnocení.

Můžete uvést odkaz na užitečné zdroje, např. adresu podpory nebo stránku s odpověďmi na časté dotazy.

Hodnocení obsahu

Náš systém hodnocení obsahu obsahuje oficiální hodnocení od [organizace IARC \(International Age Rating Coalition\)](#) a jeho cílem je pomoci vývojářům informovat uživatele o hodnocení místně relevantního obsahu.

K čemu se hodnocení obsahu používá

Hodnocení obsahu slouží k informování spotřebitelů (zejména rodičů) o potenciálně nevhodném obsahu, který se v aplikaci vyskytuje. Také pomáhá filtrovat nebo blokovat obsah na různých územích nebo konkrétním uživatelům, pokud to vyžadují právní předpisy, a určit vhodnost aplikace pro speciální programy pro vývojáře.

Jak se hodnocení obsahu přiděluje

Chcete-li získat hodnocení obsahu, musíte [ve službě Play Console vyplnit hodnoticí dotazník](#), který obsahuje otázky ohledně povahy obsahu vaší aplikace. Na základě odpovědí v dotazníku bude aplikaci přiděleno hodnocení obsahu od několika hodnoticích orgánů. Chybný popis obsahu aplikace může vést k odstranění nebo pozastavení aplikace. Proto je důležité, abyste v dotazníku hodnocení obsahu odpovídali přesně.

Chcete-li předejít tomu, aby vaše aplikace byla uvedena jako Bez hodnocení, musíte dotazník hodnocení obsahu vyplnit pro každou novou aplikaci odeslanou do služby Play Console i pro všechny stávající aplikace, které jsou na Google Play aktivní. Aplikace bez hodnocení obsahu budou z Obchodu Play odstraněny.

Pokud upravíte obsah aplikace nebo funkce, které mají vliv na odpovědi zadané do hodnoticího dotazníku, musíte do služby Play Console odeslat nový dotazník hodnocení obsahu.

Další informace o různých [hodnoticích orgánech](#) a pokyny k vyplnění dotazníku hodnocení obsahu naleznete v [centru nápovědy](#).

Odvolání proti hodnocení

Pokud s hodnocením přiděleným vaší aplikaci nesouhlasíte, můžete se odvolat přímo u hodnoticího orgánu IARC pomocí odkazu v e-mailu s certifikátem hodnocení.

Spam a minimální funkčnost

Jako minimum by aplikace uživatelům měly poskytovat alespoň základní funkčnost a zdvořilé uživatelské prostředí. Aplikace, které padají, vykazují chování neslučitelné s funkčním uživatelským prostředím nebo slouží pouze ke spamování uživatelů nebo služby Google Play, nejsou pro katalog žádným rozumným přínosem.

Spam

Nepovolujeme aplikace, které mezi uživateli nebo na Google Play šíří spam (například aplikace rozesílající nevyžádané zprávy a repetitivní nebo nekvalitní aplikace).

Spam ve zprávách

Nepovolujeme aplikace, které rozesílají SMS zprávy, e-maily nebo jiné zprávy jménem jiného uživatele, aniž by tento uživatel mohl potvrdit obsah a příjemce zprávy.

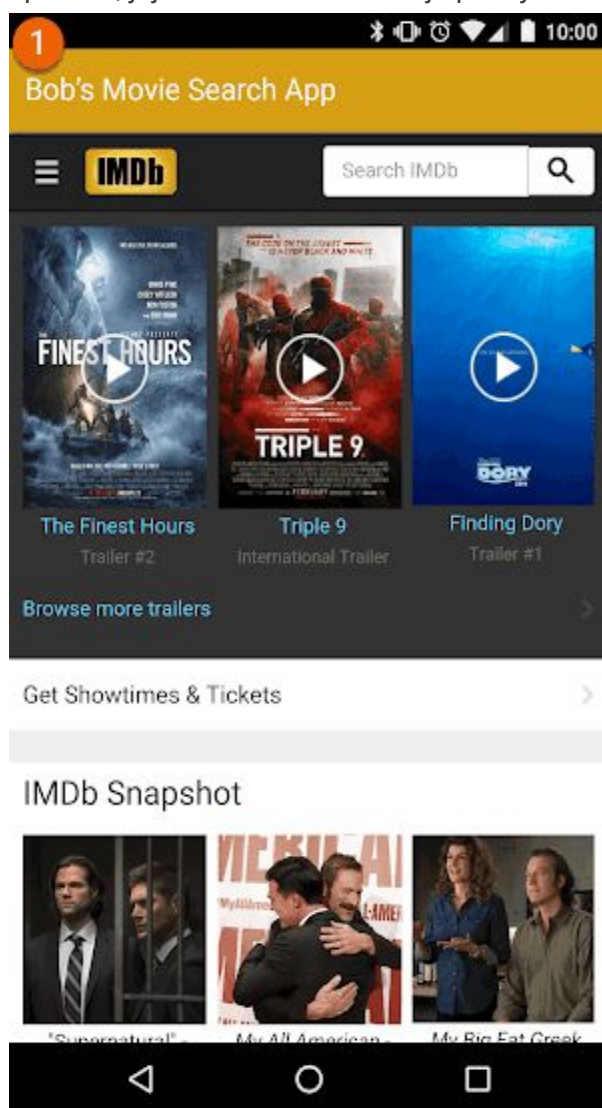
Spam zvyšující návštěvnost

Nepovolujeme aplikace, jejichž hlavním účelem je zvyšovat návštěvnost webu nebo nabízet zobrazení webu bez svolení jeho vlastníka nebo administrátora.

Aby platforma Google Play zůstala bezpečná a zdvořilá, vytvořili jsme standardy, které definují a zakazují obsah škodlivý nebo nevhodný pro uživatele.

Aplikace, jejímž hlavním účelem je odkazovat návštěvníky na určitý web a získávat kompenzaci za registrace nebo nákupy uživatelů na daném webu.

Aplikace, jejímž hlavním účelem je poskytovat zobrazení webu bez svolení:



① Tato aplikace se jmenuje „Bobova filmová databáze“ a nabízí pouze zobrazení webu IMDb.

Opakující se obsah

Nepovolujeme aplikace poskytující stejné funkce a prostředí jako jiné aplikace, které již na Google Play jsou. Aplikace by uživatelům měly poskytovat hodnotu založenou na vytváření jedinečného obsahu nebo služeb.

Aby platforma Google Play zůstala bezpečná a zdvořilá, vytvořili jsme standardy, které definují a zakazují obsah škodlivý nebo nevhodný pro uživatele.

kopírování obsahu z jiných aplikací bez přidání původního obsahu nebo hodnoty, vytvoření několika aplikací s velmi podobným obsahem a uživatelským prostředím. Pokud každá z takových aplikací nabízí malé množství obsahu, měli by vývojáři zvážit vytvoření jedné aplikace, v níž bude shrnut.

Nejsou povoleny aplikace vytvořené pomocí automatických nástrojů, průvodců či šablon a odeslané na Google Play provozovatelem příslušné služby za někoho jiného. Podobné aplikace jsou přípustné pouze v případě, že je publikuje samostatně registrovaný účet vývojáře, který patří uživateli automatického nástroje (nikoli provozovateli dané služby).

Vytvořeno pro reklamy

Nepovolujeme aplikace, jejichž primárním účelem je zobrazování reklam.

Aby platforma Google Play zůstala bezpečná a zdvořilá, vytvořili jsme standardy, které definují a zakazují obsah škodlivý nebo nevhodný pro uživatele.

aplikace, v nichž se po každé akci uživatele (např. kliknutí, přejetí prstem apod.) zobrazuje reklama.

Minimální funkčnost

Zajistěte, aby vaše aplikace poskytovala stabilní, poutavé a responzivní uživatelské prostředí.

Aby platforma Google Play zůstala bezpečná a zdvořilá, vytvořili jsme standardy, které definují a zakazují obsah škodlivý nebo nevhodný pro uživatele.

Aplikace, které nemají žádný účel ani funkci

Poruchy funkčnosti

Nepovolujeme aplikace, které padají, samy se zavírají, zamrzávají nebo vykazují jiné abnormální chování.

Aby platforma Google Play zůstala bezpečná a zdvořilá, vytvořili jsme standardy, které definují a zakazují obsah škodlivý nebo nevhodný pro uživatele.

aplikace, které nelze nainstalovat,
aplikace, které lze nainstalovat, ale nenačtou se,
aplikace, které se načtou, ale nereagují.

Naším cílem v souvislosti s okamžitými aplikacemi Android je vytvořit příjemné, bezproblémové uživatelské prostředí a zároveň zajišťovat nejvyšší standardy ochrany soukromí a zabezpečení. K dosažení tohoto cíle nám pomáhají naše zásady.

Vývojáři, kteří se rozhodnou okamžitě aplikace Android distribuovat prostřednictvím Google Play, musí kromě všech ostatních [programových zásad pro vývojáře Google Play](#) dodržovat také následující zásady.

Identita

V případě aplikací, které obsahují funkci přihlášení, musí vývojáři integrovat funkci [Smart Lock pro hesla](#).

Podpora odkazů

Vývojáři okamžitých aplikací Android musí poskytovat náležitou podporu pro odkazy na ostatní aplikace. Pokud vývojářovy okamžité aplikace nebo instalované aplikace obsahují odkazy, které lze použít ke spuštění okamžité aplikace, vývojář musí uživatele přesměrovat na příslušnou okamžitou aplikaci, nikoliv například zaznamenávat odkazy v komponentě [WebView](#).

Technické specifikace

Vývojáři musí splňovat technické specifikace okamžitých aplikací Android a požadavky společnosti Google, které mohou být čas od času upraveny, včetně těch, které jsou uvedeny v [naší veřejné dokumentaci](#).

Nabízení instalace aplikace

Okamžitá aplikace může uživateli nabízet aplikaci k nainstalování, ale nesmí to být hlavním účelem okamžité aplikace. Při nabízení instalace musí vývojář splňovat následující podmínky:

- Použít [ikonu ke stažení aplikace ve vzhledu Material Design](#) a na instalačním tlačítku použít popisek Instalovat.

- Mít v okamžité aplikaci obsaženy maximálně dvě až tři výzvy k instalaci.

- K prezentování výzvy k instalaci uživatelům nepoužívat banner ani jinou techniku podobnou reklamám.

Další podrobnosti o okamžitých aplikacích a pokyny k uživatelskému rozhraní naleznete v [doporučených postupech k uživatelskému prostředí](#).

Změna stavu zařízení

Okamžité aplikace nesmí v zařízení uživatele provádět změny, které trvají déle než relace okamžité aplikace. Například nesmí změnit tapetu uživatele nebo vytvořit widget na ploše.

Viditelnost aplikace

Vývojáři musí zajistit, aby okamžité aplikace byly pro uživatele viditelné a uživatel si byl po celou dobu vědom, že je v jeho zařízení spuštěna okamžitá aplikace.

Identifikátory zařízení

Okamžité aplikace mají zakázáno používat identifikátory zařízení, které (1) přetrvávají i po ukončení okamžité aplikace a (2) uživatel je nemůže resetovat. Patří sem (mimo jiné):

- sériové číslo sestavení,
- adresy MAC síťových čipů,

IMEI, IMSI.

Okamžité aplikace mohou používat telefonní číslo, pokud bude získáno v rámci oprávnění uděleného při běhu aplikace. Vývojář se nesmí pokoušet pomocí těchto identifikátorů nebo jiných prostředků získat otisky prstů uživatele.

Síťový provoz

Síťový provoz pocházející z okamžité aplikace musí být šifrován pomocí protokolu TLS, jako například HTTPS.

Rodiny

Google Play nabízí platformu, na které vývojáři mohou prezentovat kvalitní a věkově přiměřený obsah pro celou rodinu. U aplikací, které odesíláte do programu Pro celou rodinu, a aplikací zacílených na děti, které odesíláte do Obchodu Google Play, jste povinni zajistit, aby byly vhodné pro děti a byly v souladu se všemi relevantními zákony.

[Přečtěte si další informace o procesu pro rodiny a projděte si interaktivní kontrolní seznam v kurzu Academy for App Success.](#)

Navrhování aplikací pro děti a rodiny

Technologie se stále více používají jako nástroj ke zlepšení rodinného života a rodiče hledají bezpečný a kvalitní obsah, který by mohli sdílet se svými dětmi. Aplikace můžete navrhovat speciálně pro děti, ale mohou také pouze přitahovat jejich pozornost. Google Play vám chce pomoci zajistit, aby vaše aplikace byla bezpečná pro všechny uživatele, včetně rodin.

Slovo „děti“ může mít v různých regionech a kontextech různý význam. Je důležité, abyste se svým právníkem prokonzultovali, jaké povinnosti či věková omezení se na vaši aplikaci mohou vztahovat. Sami nejlépe víte, jak vaše aplikace funguje. Spoléháme proto na vás, že nám pomůžete zajistit, aby aplikace na Google Play byly bezpečné pro rodiny.

Aplikace navržené speciálně pro děti je nutné zařadit do programu Pro celou rodinu. Pokud však děti tvoří jen část cílového publika aplikace, účast v programu Pro celou rodinu na Google Play je skvělý způsob, jak aplikaci nabídnout správným uživatelům. I v případě, že se do programu Pro celou rodinu nezapojíte, musíte splňovat požadavky zásad Google Play pro rodiny uvedené níže, všechny ostatní [programové zásady služby Google Play pro vývojáře](#) a [Distribuční smlouvu pro vývojáře](#).

Požadavky na Play Console

Cílové publikum a obsah

V sekci [Cílové publikum a obsah](#) ve službě Google Play Console musíte před publikováním aplikace v seznamu věkových skupin vybrat cílové publikum. Pokud do aplikace zahrnete obrázky a výrazy, které by mohly být považovány za zacílené na děti, může to mít vliv na posouzení deklarovaného cílového publika ve službě Google Play bez ohledu na to, co uvedete v Google Play Console. Služba Google Play si vyhrazuje právo provést vlastní kontrolu uvedených informací o aplikaci s cílem zjistit, zda uvádíte správné cílové publikum.

Pokud vyberete cílové publikum zahrnující pouze dospělé, ale společnost Google usoudí, že aplikace kromě nich cílí i na děti, budete moci souhlasit s přidáním varovného štítku, podle kterého uživatelé jasně poznají, že aplikace není určená pro děti.

Více než jednu věkovou skupinu byste jako cílové publikum aplikace měli vybrat jen v případě, že jste aplikaci navrhli pro uživatele z vybraných věkových skupin a zajistili, aby pro ně byla vhodná. Příklad: U aplikací určených pro batolata a předškolní děti by měla být vybrána pouze cílová věková skupina Věk do 5 let. Pokud je aplikace určena pro konkrétní školní ročník, vyberte věkovou skupinu, která mu nejlépe odpovídá. Věkové skupiny zahrnující dospělé i děti byste měli vybrat pouze v případě, že jste aplikaci opravdu navrhli pro všechny věkové skupiny.

Aktualizace v sekci Cílové publikum a obsah

Informace o aplikaci v sekci Cílové publikum a obsah v Google Play Console můžete kdykoliv aktualizovat. Aby se tyto informace projevily na Google Play, je vyžadována [aktualizace aplikace](#). Změny provedené v této sekci Google Play Console však mohou být ještě před vydáním aktualizace zkontrolovány, zda jsou v souladu se zásadami.

Pokud u aplikace měníte cílovou věkovou skupinu nebo v ní začínáte používat aplikace či nákupy v aplikaci, důrazně doporučujeme informovat o tom stávající uživatele. Můžete to provést prostřednictvím sekce Novinky na stránce záznamu v obchodě nebo prostřednictvím oznámení v aplikaci.

Uvedení nepravdivých údajů v Play Console

Uvedení nepravdivých informací o aplikaci v Play Console, včetně informací v sekci Cílové publikum a obsah, může vést k odstranění nebo pozastavení aplikace. Je proto nutné uvést přesné údaje.

Požadavky zásad pro rodiny

Pokud cílové publikum aplikace zahrnuje děti, musíte splnit následující požadavky. Pokud je nesplníte, může to vést k odstranění nebo pozastavení aplikace.

1. Obsah aplikace: Obsah aplikace přístupný dětem musí být vhodný pro děti.
2. Odpovědi v Google Play Console: Musíte pravdivě odpovědět na otázky ohledně aplikace v Google Play Console a aktualizovat je tak, aby přesně reflektovaly veškeré změny aplikace.

3. Reklamy: Pokud se v aplikaci zobrazují reklamy dětem nebo uživatelům neznámého věku, musíte:
 - k zobrazování reklam těmto uživatelům používat jen reklamní sady SDK certifikované službou Google Play,
 - zajistit, aby reklamy zobrazované těmto uživatelům nebyly zájmově orientované a nejednalo se o remarketing,
 - zajistit, aby reklamy zobrazované těmto uživatelům prezentovaly obsah vhodný pro děti,
 - zajistit, aby reklamy zobrazované těmto uživatelům splňovaly požadavky na formát reklam pro rodiny,
 - zajistit soulad s veškerými příslušnými právními předpisy a oborovými standardy ohledně inzerce určené pro děti.
4. Shromažďování údajů: Pokud v aplikaci shromažďujete od dětí **osobní či citlivé údaje** (včetně shromažďování prostřednictvím API a sad SDK, které aplikace volá nebo využívá), musíte o tom uživatele informovat. Mezi citlivé údaje od dětí patří mimo jiné ověřovací informace, údaje z mikrofonu a kamery, údaje o zařízení, Android ID, údaje o využití reklam a inzertní ID.
5. Rozhraní API a sady SDK: Musíte zajistit, aby vaše aplikace případná rozhraní API a sady SDK implementovala správně.
 - Aplikace, které cílí výhradně na děti, nesmějí obsahovat žádná rozhraní API ani sady SDK, které nejsou schváleny k použití ve službách určených pro děti.
 - Nesmějí například obsahovat přihlášení přes Google (ani žádnou jinou službu Google API, která používá data přidružená k účtu Google), herní služby Google Play ani žádnou jinou službu API, která k přihlášení a ověření používá technologii OAuth.
 - Aplikace, které cílí na děti i starší publikum by neměly implementovat rozhraní API ani sady SDK, které nejsou schváleny k použití ve službách určených pro děti.
 - Mohou je používat pouze za **neutrálním věkovým filtrem** nebo implementovat způsobem, který nevede ke shromažďování dat od dětí (např. přihlášení přes Google poskytovat jako volitelnou funkci). Všichni uživatelé musejí mít přístup k aplikaci a rozumné míře její funkčnosti.
6. Zásady ochrany soukromí: Na stránce záznamu v obchodu aplikace musíte publikovat odkaz na její zásady ochrany soukromí. Dokud je aplikace v obchodě k dispozici, musí být odkaz stále aktualizován a musí odkazovat na zásady ochrany soukromí, které mimo jiné přesně popisují, jak aplikace shromažďuje a používá data.
7. Zvláštní omezení:
 - Pokud aplikace používá rozšířenou realitu, musíte při spuštění části s rozšířenou realitou ihned zobrazit bezpečnostní upozornění. Upozornění musí obsahovat:
 - sdělení ohledně důležitosti dohledu rodičů,
 - připomenutí, že je potřeba dávat pozor na fyzická nebezpečí v reálném světě (například sledovat okolí).
 - Aplikace nesmí vyžadovat použití zařízení, které by neměly používat děti (např. Daydream, Oculus).

8. Soulad s právními předpisy: Musíte zajistit, aby aplikace, včetně rozhraní API nebo sad SDK, které volá nebo využívá, byla v souladu se [zákonem USA o ochraně soukromí dětí na internetu \(COPPA\)](#), [obecným nařízením EU o ochraně osobních údajů \(GDPR\)](#) a dalšími příslušnými zákony či předpisy.

Aby platforma Google Play zůstala bezpečná a zdvořilá, vytvořili jsme standardy, které definují a zakazují obsah škodlivý nebo nevhodný pro uživatele.

aplikace inzerované v záznamu v obchodu jako určené pro děti, jejichž obsah je vhodný pouze pro dospělé,
aplikace, které implementují rozhraní API, jejichž smluvní podmínky zakazují použití v aplikacích určených pro děti,
aplikace, které idealizují konzumaci alkoholu, tabákových výrobků nebo kontrolovaných látek,
aplikace, které obsahují hazardní hraní nebo jeho simulaci,
aplikace s násilím, krvavými scénami nebo šokujícím obsahem nevhodným pro děti,
seznamovací aplikace nebo aplikace nabízející sexuální či manželské poradenství.
aplikace, které dětem zobrazují reklamy pouze pro dospělé.

Program Pro celou rodinu

Aplikace navržené speciálně pro děti je nutné zařadit do programu Pro celou rodinu. O zařazení do programu Pro celou rodinu můžete požádat i v případě, že je vaše aplikace určená pro všechny, včetně dětí a rodin.

Před přijetím do tohoto programu musí aplikace kromě podmínek uvedených v [programových zásadách služby Google Play pro vývojáře](#) a [distribuční smlouvě pro vývojáře](#) splnit také všechny požadavky zásad pro rodiny a podmínky na způsobilost k účasti v programu Pro celou rodinu.

Další informace o procesu odeslání aplikace k zařazení do programu zobrazíte [kliknutím sem](#).

Způsobilost pro program

Všechny aplikace v programu Pro celou rodinu musejí mít obsah (včetně reklam) relevantní a vhodný pro děti a musejí splňovat všechny následující požadavky. Aplikace přijaté do programu Pro rodiny musejí po celou dobu splňovat všechny požadavky programu. Google Play si vyhrazuje právo podle vlastního uvážení odmítnout nebo odstranit libovolnou aplikaci, o které usoudíme, že pro program Pro celou rodinu není vhodná.

Požadavky programu Pro celou rodinu

1. Aplikace musí mít v systému ESRB hodnocení Všichni nebo Všichni od 10 let (nebo ekvivalentní).
2. V dotazníku hodnocení obsahu v Google Play Console musíte pravdivě uvést interaktivní prvky aplikace, včetně informací o tom, zda:
 - uživatelé mohou vzájemně komunikovat nebo si vyměňovat informace,

aplikace sdílí s třetími stranami osobní údaje poskytované uživateli,
aplikace sdílí s ostatními uživateli informace o fyzické poloze uživatele.

3. Pokud vaše aplikace používá rozhraní [Android Speech API](#), její parametr RecognizerIntent.EXTRA_CALLING_PACKAGE musí být nastaven na její PackageName.
4. Aplikace smějí používat pouze [reklamní sady SDK certifikované pro Google Play](#).
5. Aplikace navržené speciálně pro děti nesmějí žádat o oprávnění pro přístup k poloze.
6. Aplikace žádající o přístup k rozhraní Bluetooth musejí používat [Správce doprovodných zařízení \(CDM\)](#) (kromě aplikací, jež cílí pouze na verze operačního systému zařízení, které se Správce doprovodných zařízení nejsou kompatibilní).

Zde je několik příkladů běžných aplikací, které nesplňují podmínky zařazení do programu:

aplikace, které mají v systému ESRB hodnocení Všichni, ale obsahují reklamy na hazardní hry,
aplikace pro rodiče nebo opatrovatele (např. aplikace na evidenci kojení, průvodce vývojem dítěte),
příručky pro rodiče nebo aplikace pro správu zařízení určené jen pro rodiče nebo opatrovatele.

Kategorie

Po přijetí do programu Pro celou rodinu můžete zvolit druhou rodinnou kategorii, která vaši aplikaci popisuje. Pro aplikace v programu Pro celou rodinu jsou k dispozici následující kategorie:

Akce a adventury: Aplikace a hry zaměřené na akci, od jednoduchých závodních her, přes pohádkové adventury až po jiné aplikace a hry navržené s cílem vytvářet vzrušení.

Pro chytré hlavy: Hry, u kterých uživatel musí přemýšlet, např. hlavolamy, logické hry, kvízy a jiné hry, u nichž je potřeba zapojit paměť, inteligenci nebo logiku.

Kreativita: Aplikace a hry, které rozvíjí kreativitu, např. kreslení, malování, programování a další aplikace a hry, ve kterých lze tvořit.

Vzdělávání: Aplikace a hry navržené ve spolupráci s odborníky na vzdělávání (např. učitelé, vzdělávací instruktoři, vědci) s cílem rozvíjet akademické, sociálně-emoční, fyzické a kreativní dovednosti, ale také základní životní dovednosti, kritické myšlení a schopnost řešit problémy.

Hudba a video: Aplikace a hry s hudebním prvkem nebo videem, tj. vše od simulátorů hraní na hudební nástroje po aplikace, které prezentují videa a hudební obsah.

Hraní rolí: Aplikace a hry, ve kterých uživatel může hrát nějakou roli, například roli kuchaře, ošetřovatele, prince či princezny, hasiče, policisty nebo fiktivní postavy.

Reklamy a zpeněžení

Níže uvedené zásady se vztahují na veškerou inzerci (včetně reklam na vaše aplikace a aplikace třetích stran), nabídky nákupů v aplikaci a veškerý další komerční obsah (jako je placený product placement) zobrazovaný uživatelům aplikací, na které se vztahují požadavky zásad pro rodiny nebo programu Pro celou rodinu. Veškerá inzerce, nabídky nákupů v aplikaci a komerční obsah v těchto aplikacích musí být v souladu s příslušnými právními předpisy a nařízeními (včetně relevantních zásad samoregulace a standardů v odvětví).

Google Play si vyhrazuje právo podniknout kroky vůči aplikacím, které používají příliš agresivní obchodní taktiky.

Podmínky pro formát reklam

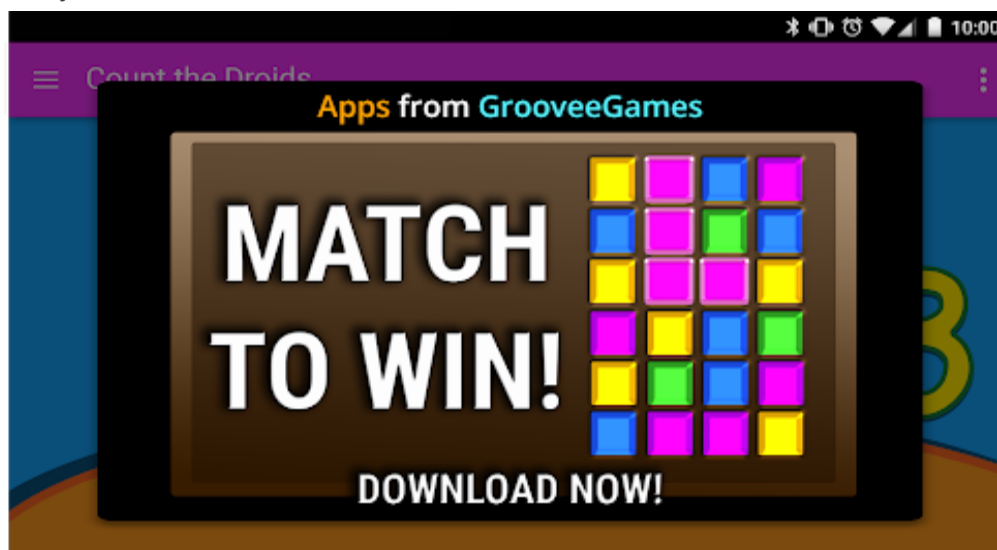
Reklamy a nabídky nákupů v aplikacích nesmí mít klamavý obsah a nesmí být navrženy způsobem, který by měl za následek neúmyslná kliknutí dětských uživatelů. Jsou zakázány následující praktiky:

- podmiňování přístupu k obsahu zhlédnutím reklamy,
- reklamy, které narušují běžné používání aplikace a které nelze zavřít po uplynutí 5 sekund,
- zobrazování vsunutých reklam nebo nabídek nákupů v aplikaci ihned po spuštění aplikace,
- používání několika umístění reklam na stránce,
- zobrazování reklam nebo nabídek nákupů v aplikaci, které nelze jasně odlišit od obsahu aplikace,
- používání šokujících nebo emocionálně manipulativních taktik s cílem přimět uživatele ke zhlédnutí reklam či nákupů v aplikaci,
- nerozlišování virtuální herní měny a reálných peněz u nákupů v aplikacích.

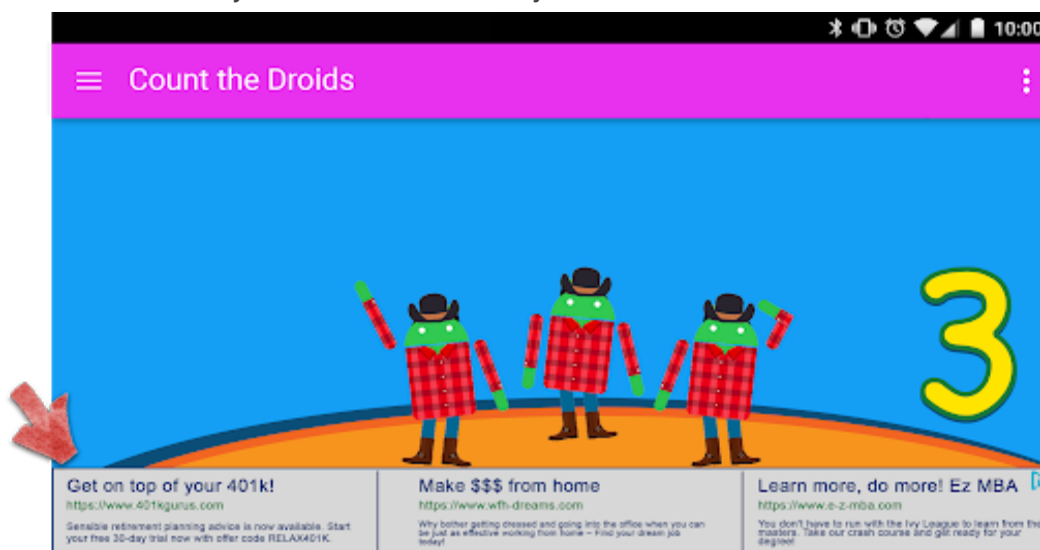
Aby platforma Google Play zůstala bezpečná a zdvořilá, vytvořili jsme standardy, které definují a zakazují obsah škodlivý nebo nevhodný pro uživatele.

Reklamy, které uživateli uhýbají, když se je prstem pokouší zavřít

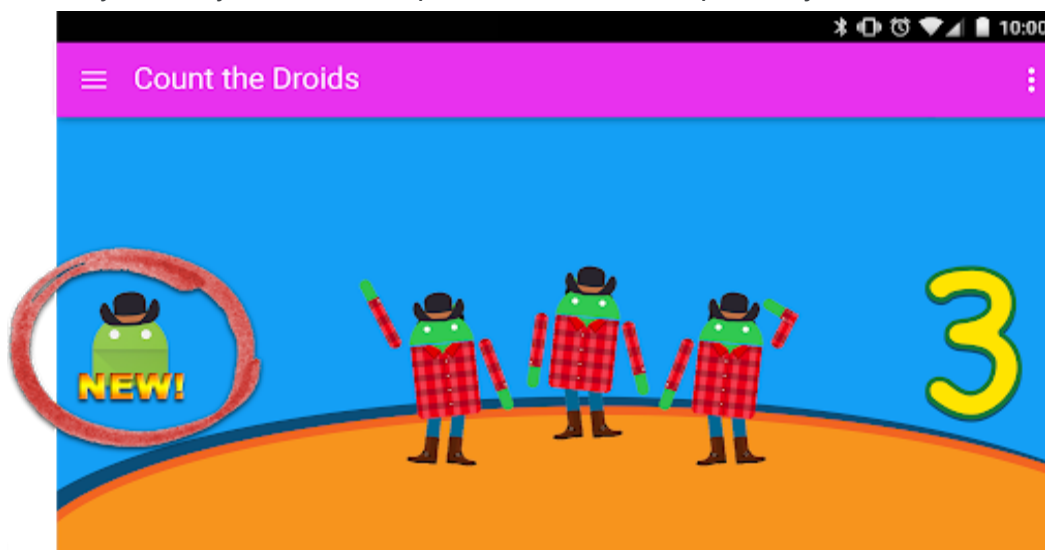
Reklamy, které zabírají většinu obrazovky zařízení a neposkytují uživateli jasnou možnost zavření, jako na obrázku níže:



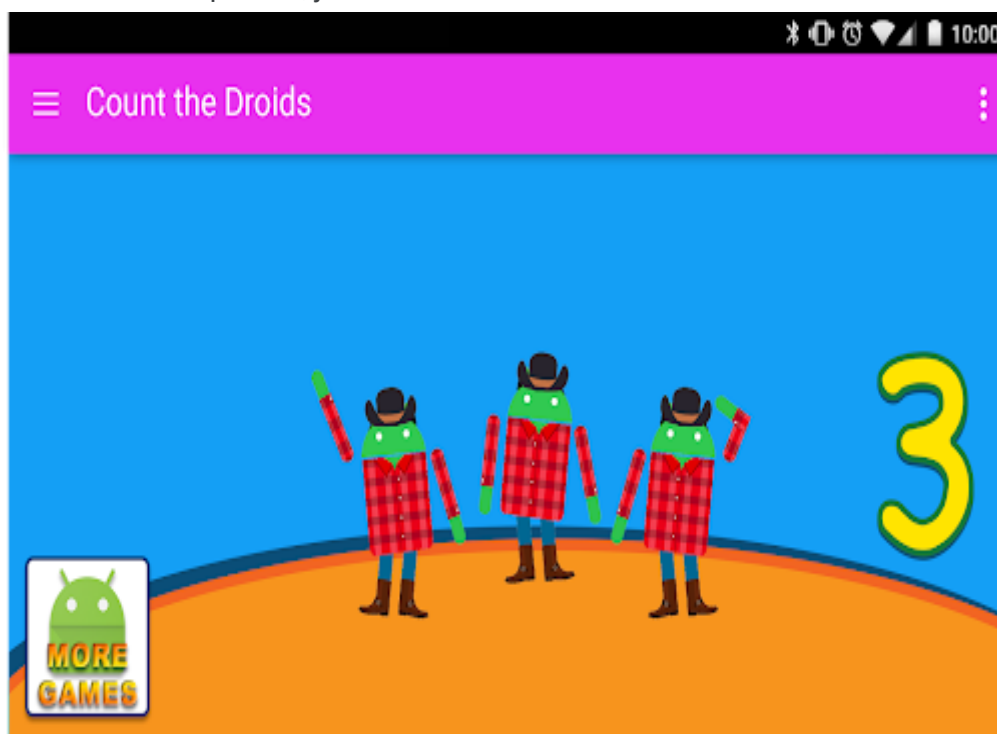
Bannerové reklamy s několika nabídkami jako na obrázku níže:



Reklamy, které by uživatel mohl považovat za obsah aplikace, jako na obrázku níže:



Tlačítka nebo reklamy propagující jiné vaše záznamy v obchodě Google Play, které nelze rozlišit od obsahu aplikace, jako na obrázku níže:



Zde je několik příkladů nevhodného obsahu reklam, který byste neměli zobrazovat dětem.

Nevhodný mediální obsah: Reklamy na televizní pořady, filmy, hudební alba a další mediální produkty, které nejsou vhodné pro děti.

Nevhodné videohry a software ke stažení: Reklamy na software ke stažení a elektronické videohry, které nejsou vhodné pro děti.

Kontrolované nebo škodlivé látky: Reklamy na alkohol, tabák, kontrolované látky nebo jakékoliv jiné škodlivé látky.

Hazardní hry: Reklamy na simulované hazardní hraní, soutěže nebo sázky (včetně bezplatných).

Obsah pro dospělé a se sexuálním podtextem: Reklamy s obsahem, který je sexuálního charakteru, má sexuální podtext nebo není vhodný pro děti.

Randění a seznamky: Reklamy na seznamovací weby.

Násilný obsah: Reklamy s násilným nebo explicitním obsahem, které nejsou vhodné pro děti.

Sady SDK pro reklamy

K zobrazování reklam dětem lze používat jen [reklamní sady SDK certifikované službou Google Play](#). Aplikace v programu Pro celou rodinu mohou používat pouze reklamní sady SDK certifikované službou Google Play. U aplikací, které cílí také na dospělé uživatele, lze necertifikované reklamní sady SDK použít v případě, že je v aplikaci implementován [neutrální věkový filtr](#) a pomocí necertifikovaných reklamních sítí se reklamy zobrazují pouze uživatelům, o nichž je známo, že jsou dospělí.

Další podrobnosti o těchto požadavcích a aktuální seznam schválených reklamních sad SDK najdete na stránce [Reklamy v programu Pro celou rodinu](#).

Jestliže používáte službu AdMob, další informace o jejích produktech naleznete v [centru nápovědy AdMob](#).

Jste odpovědní za to, aby aplikace splňovala všechny požadavky ohledně reklam, nákupů v aplikacích a komerčního obsahu. Chcete-li získat další informace o obsahových zásadách a reklamních postupech svých poskytovatelů reklamních sad SDK, kontaktujte přímo je.

Nákupy v aplikaci

V aplikacích zařazených do programu Pro celou rodinu bude služba Google Play před všemi nákupy v aplikaci každého uživatele znovu ověřovat. Toto opatření má za cíl zajistit, aby nákupy schvalovali finančně odpovědné osoby, nikoliv děti.

Vynucování

Vyhnout se porušení zásad je vždy lepší, než ho řešit. Když už však k porušení zásad dojde, snažíme se vývojářům pomoci zjistit příčinu, aby mohli chybu napravit a zajistit, že bude aplikace zásady dodržovat. Pokud se vám [zobrazuje upozornění na porušení zásad](#) nebo se chcete zeptat, [jak při porušení zásad postupovat](#), kontaktujte nás.

Rozsah zásad

Naše zásady se týkají veškerého obsahu, který vaše aplikace zobrazuje nebo na který odkazuje, včetně veškerých reklam zobrazovaných uživatelům a obsahu vytvářeného uživateli, který aplikace hostuje nebo na který odkazuje. Vztahují se také na jakýkoliv obsah z vašeho účtu vývojáře, který se veřejně zobrazuje na Google Play, včetně vašeho názvu vývojáře a vstupní stránky vašeho zveřejněného webu vývojáře.

Nepovolujeme aplikace, které uživatelům umožňují instalovat do zařízení jiné aplikace. Aplikace, které poskytují přístup bez instalace k jiným aplikacím, hrám nebo softwaru (včetně funkcí a služeb třetích stran), musí zajistit, aby veškerý takto poskytnutý obsah byl v souladu se [zásadami Google Play](#). U tohoto obsahu může docházet k dodatečným kontrolám dodržování zásad.

Definované termíny použité v tomto dokumentu mají stejný význam jako v [distribuční smlouvě pro vývojáře](#). Kromě zajištění souladu s těmito zásadami musí být obsah aplikace také ohodnocen podle našich [pokynů pro hodnocení obsahu](#).

Aplikace, které nejsou vhodné pro široké publikum nebo u koncových uživatelů vzbuzují špatný dojem, nelze na Google Play propagovat. Pokud jsou však v souladu se zásadami a distribuční smlouvou pro vývojáře, budou na Google Play i nadále k dispozici.

Společnost Google si vyhrazuje právo zahrnout aplikace na Google Play nebo je odstranit. Můžeme podniknout akci na základě různých faktorů, mezi něž patří mimo jiné podezření na škodlivé chování nebo vysoké riziko zneužití. Riziko zneužití identifikujeme podle indicií, jako je porušení zásad v minulosti, zpětná vazba uživatelů nebo použití populárních značek, postav nebo jiných položek.

Proces uplatňování zásad

Pokud aplikace porušuje naše zásady, bude z Google Play odstraněna a vy obdržíte e-mailem oznámení s konkrétními informacemi, proč byla aplikace odstraněna. Opakovaná nebo závažná porušení zásad (např. malware, podvody a aplikace, které mohou ohrozit uživatele nebo poškodit zařízení) nebo [distribuční smlouvy pro vývojáře](#) budou mít za následek zrušení příslušného účtu (případně i účtů souvisejících).

Upozorňujeme, že administrativní oznámení a oznámení o odstranění aplikace nemusí uvádět všechna porušení zásad, ke kterým došlo v jedné či ve víceru vašich aplikacích. Vývojáři nesou odpovědnost za vyřešení všech uvedených problémů, ale také se očekává, že věnují zvýšenou pozornost tomu, aby k žádnému porušení zásad nedošlo ani ve zbytku aplikace. Pokud vývojář porušení zásad nevyřeší, můžeme podniknout další kroky, např. trvale odstranit aplikace nebo zrušit účet.

Správa a hlášení porušení zásad

Pokud máte dotazy nebo nejasnosti ohledně odstranění hodnocení nebo komentáře uživatele, můžete nás kontaktovat prostřednictvím níže uvedených zdrojů nebo skrze [centrum nápovědy Google Play](#). Neposkytujeme však právní poradenství. Pokud ho potřebujete, obraťte se na právního zástupce.

[Ověřování aplikací a odvolání](#)

[Nahlášení porušení zásad](#)

[Kontaktování Google Play ohledně zrušení účtu nebo odstranění aplikace](#)

[Včasná varování](#)

[Nahlášení nevhodných aplikací a komentářů](#)

[Moje aplikace byla odstraněna z Google Play](#)

[Kdy dochází ke zrušení účtu vývojáře pro Google Play](#)

[Developer Distribution Agreement](#)