

Programové zásady pro vývojáře (platné od 1. března 2021)

Pojďme společně vytvořit nejdůvěryhodnější zdroj aplikací a her na světě

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 prostřednictvím Google Play budeme společně nabízet nejnovější a nejdůvěryhodnější aplikace na světě více než miliardy uživatelů. Naše zásady si můžete prohlédnout níže.

Zakázaný obsah

Pomocí Google Play denně vyhledávají aplikace a hry lidé z celého světa. Před publikováním každé aplikace si položte otázku, zda je aplikace pro Google Play vhodná a zda je v souladu s místními právními předpisy.

Ohrožení dětí

Aplikace s obsahem, který sexualizuje nezletilé, budou z obchodu okamžitě odstraněny. Patří sem mimo jiné aplikace, které propagují pedofilii nebo nevhodnou interakci s nezletilými (např. osahávání).

Nejsou povoleny ani aplikace, které pro děti sice přitažlivé jsou, ale obsahují motivy určené pouze dospělým, například aplikace s nadměrným násilím nebo s krvavými scénami, nebo aplikace, které zobrazují škodlivé či nebezpečné aktivity nebo k nim navádějí. Povoleny nejsou ani aplikace propagující negativní pohled na tělo nebo na vlastní obraz, například aplikace, které pro zábavu zobrazují na fyzické podobě osoby účinky plastických operací, hubnutí nebo jiných kosmetických vylepšení.

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

Nevhodný obsah

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

Sexuální obsah a vulgární výrazy

Nepovolujeme aplikace, které zahrnují či propagují sexuální obsah nebo vulgární výrazy (např. pornografii), ani obsah či 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.

Příklady běžných porušení zásad:

- Vyobrazení sexuální nahoty nebo sexuálně sugestivních póz, na nichž je osoba nahá, rozostřená, jen minimálně oblečená nebo se nachází v prostředí, kde by její oblečení ve veřejném kontextu nebylo přijatelné.
- Vyobrazení, animace nebo ilustrace sexuálních aktivit, sexuálně sugestivních póz nebo sexuální vyobrazení částí těla.
- Obsah, který zobrazuje nebo funguje jako sexuální pomůcka, sexuální návod, nezákonné sexuální téma nebo fetiš.
- Obscéní či sprostý obsah (např. obsah, který může v záznamu v obchodu nebo v aplikaci obsahovat vulgární výrazy, urážky, explicitní text, sexuální nebo jen dospělým určená klíčová slova).
- 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.
- Aplikace, které lidi ponižují nebo deklasují.

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.

V souladu s místními zákony a jinými právními předpisy mohou být v některých zemích blokovány i aplikace s obsahem vzdělávacího, dokumentárního, vědeckého nebo uměleckého charakteru, které souvisí s nacisty.

Příklady běžných porušení zásad:

- Obsah nebo projev prohlašující, že je určitá chráněná skupina nelidská, podřadná nebo si zasluhuje nenávisť.
- Aplikace, které obsahují nenávistné projevy, stereotypy nebo teorie, že příslušníci určité chráněné skupiny mají negativní vlastnosti (např. že jsou zákeřní, zkažení, zlí apod.) nebo explicitně či implicitně tvrdí, že taková skupina představuje hrozbu.
- Obsah nebo projevy, které se ostatní lidi pokouší přesvědčit k nenávisti nebo diskriminaci vůči členům chráněné skupiny.
- Obsah, který propaguje symboly nenávisti, jako jsou vlajky, symboly, odznaky, výstroj nebo prvky související se skupinami šířícími nenávisť.

Násilí

Nepovolujeme aplikace, které zobrazují bezdůvodné násilí či jiné nebezpečné aktivity, ani obsah, který takovému chování napomáhá. Aplikace, které ukazují fiktivní násilí v kontextu hry (např. v kreslených hrách), lovu nebo rybaření, jsou obecně povoleny.

Příklady běžných porušení zásad:

- Náзорé vyobrazení nebo popis realistického násilí nebo násilného vyhrožování člověku nebo zvířeti.
- Aplikace, které propagují sebepoškozování, sebevraždu, šikanu, obtěžování, poruchy příjmu potravy, hry spojené s dušením nebo jiné aktivity spojené s rizikem vážného zranění nebo úmrtí.

Teroristický obsah

Teroristickým organizacím nedovolujeme publikovat aplikace na Google Play 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. Aplikace s obsahem spojeným s citlivou událostí jsou obecně povoleny, pokud má obsah vzdělávací, dokumentární, vědeckou nebo uměleckou hodnotu, případně se snaží uživatele informovat nebo upozornit.

Příklady běžných porušení zásad:

- 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 vyhrožování nebo uživatele obtěžují či zastrašují, ani aplikace, které takové chování podporují.

Příklady běžných porušení zásad:

- 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.

Příklady běžných porušení zásad:

- Umožnění objednávek marihuany prostřednictvím nákupního košíku v aplikaci.
- Pomáhání uživatelům s dohodnutím dodávky nebo vyzvednutí marihuany.
- Zprostředkovávání prodeje produktů, které obsahují THC (tetrahydrokanabinol), včetně CBD olejů a podobných výrobků s obsahem THC.

Tabákové výrobky a alkohol

Nepovolujeme aplikace, které umožňují prodej tabákových výrobků (včetně elektronických cigaret a vaporizérů) nebo podporují nezákonné či nevhodné použití alkoholu či tabákových výrobků.

Příklady běžných porušení zásad:

- Vyobrazení nebo propagace konzumace alkoholu či tabáku nezletilými nebo prodej 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, splátkovém kalendáři, 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, které poskytují osobní půjčky (například aplikace, které přímo nabízejí půjčky, oslovují potenciální zákazníky nebo uživatele spojují s externími poskytovateli půjček) musí v metadatech aplikace uvést 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.

- zásady ochrany osobních údajů, které komplexně popisují přístup k osobním a citlivým uživatelským údajům a jejich shromažďování, používání a sdílení.

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“).

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.

Příklad běžného porušení zásad:

The screenshot shows the Easy Loans app interface. At the top, there's a navigation bar with a back arrow and a menu icon. Below it, the app logo 'Easy Loans' is displayed with the tagline 'offers in app purchases'. A green 'Install' button is visible. The main content area starts with the question 'Are you looking for a speedy loan?' followed by a description: 'Easy Loans Finance can help you get cash in your bank account in an hour!'. A list of bullet points follows: 'Get cash sent to your bank account!', 'Safe and easy', 'Great short-term rate', 'Fast lender approval', 'Easy to use', 'Loan delivered in an hour', and 'Download our app and get cash easy!'. A red box labeled 'Violations' points to a red box containing the following text: 'No minimum and maximum period for repayment', 'Doesn't disclose Maximum Annual Percentage Rate (APR), which generally includes interest rate plus fees and other costs for a year, or similar other rate calculated consistently with local law', and 'No representative example of the total cost of the loan, including all applicable fees'.

Hazardní hry, hry a soutěže se skutečnými penězi

Povolujeme hazardní hry se skutečnými penězi, reklamy související s hazardními hrami se skutečnými penězi a aplikace pro denní fantasy sporty, které splňují určité požadavky.

Hazardní aplikace

S ohledem na omezení a dodržování všech zásad Google Play povolujeme aplikace, které umožňují nebo usnadňují online hazardní hry v zemích uvedených v tabulce níže, pokud vývojář [projde procesem žádosti](#) pro hazardní aplikace distribuované na Google Play, je schváleným státním provozovatelem a/nebo je registrován jako licencovaný provozovatel u příslušného státního úřadu pro hazardní hry v uvedené zemi a předloží platnou provozní licenci pro uvedenou zemi na typ online hazardu, který chce nabízet.

Povolujeme pouze licencované nebo autorizované hazardní aplikace, které obsahují následující typy produktů online hazardu (v tabulce níže naleznete konkrétní typy hazardních produktů povolené v jednotlivých zemích):

- Online kasinové hry
- Loterie
- Sportovní sázení
- Denní fantasy sporty

Austrálie

Souhrn	Podrobnosti
--------	-------------

Souhrn	Podrobnosti
Povoleno s omezeními	S ohledem na výše uvedené požadavky na aplikace a licencování jsou povoleny aplikace s následujícími typy hazardních produktů: • Sportovní sázení • Loterie • Denní fantasy sporty

Belgie

Souhrn	Podrobnosti
Povoleno s omezeními	S ohledem na výše uvedené požadavky na aplikace a licencování jsou povoleny aplikace s následujícími typy hazardních produktů: • Online kasinové hry • Sportovní sázení • Loterie (pouze státní provozovatelé)

Brazílie

Souhrn	Podrobnosti
Povoleno s omezeními	S ohledem na výše uvedené požadavky na aplikace a licencování jsou povoleny aplikace s následujícími typy hazardních produktů: • Loterie (pouze pro schválené aplikace publikované bankou Caixa Econômica Federal) • Sportovní sázení (pouze koňské dostihy)

Kanada

Souhrn	Podrobnosti
Povoleno s omezeními	S ohledem na výše uvedené požadavky na aplikace a licencování jsou povoleny aplikace s následujícími typy hazardních produktů: • Internetové kasino (pouze státní provozovatelé) • Sportovní sázení (pouze státní provozovatelé) • Loterie (pouze státní provozovatelé)

Kolumbie

Souhrn	Podrobnosti
Povoleno s omezeními	S ohledem na výše uvedené požadavky na aplikace a licencování jsou povoleny aplikace s následujícími typy hazardních produktů: • Internetové kasino • Sportovní sázení • Loterie (pouze státní provozovatelé)

Dánsko

Souhrn	Podrobnosti
--------	-------------

Souhrn	Podrobnosti
Povoleno s omezeními	S ohledem na výše uvedené požadavky na aplikace a licencování jsou povoleny aplikace s následujícími typy hazardních produktů: • Internetové kasino • Sportovní sázení • Loterie • Denní fantasy sporty

Finsko

Souhrn	Podrobnosti
Povoleno s omezeními	S ohledem na výše uvedené požadavky na aplikace a licencování jsou povoleny aplikace s následujícími typy hazardních produktů: • Internetové kasino (pouze státní provozovatelé) • Sportovní sázení (pouze státní provozovatelé) • Loterie (pouze státní provozovatelé)

Francie

Souhrn	Podrobnosti
Povoleno s omezeními	S ohledem na výše uvedené požadavky na aplikace a licencování jsou povoleny aplikace s následujícími typy hazardních produktů: • Internetové kasino • Sportovní sázení • Loterie (pouze státní provozovatelé)

Německo

Souhrn	Podrobnosti
Povoleno s omezeními	S ohledem na výše uvedené požadavky na aplikace a licencování jsou povoleny aplikace s následujícími typy hazardních produktů: • Sportovní sázení • Loterie (pouze státní provozovatelé)

Irsko

Souhrn	Podrobnosti
Povoleno s omezeními	S ohledem na výše uvedené požadavky na aplikace a licencování jsou povoleny aplikace s následujícími typy hazardních produktů: • Internetové kasino • Sportovní sázení • Loterie (pouze státní či charitativní provozovatelé)

Japonsko

Souhrn	Podrobnosti
--------	-------------

Souhrn	Podrobnosti
Povoleno s omezeními	S ohledem na výše uvedené požadavky na aplikace a licencování jsou povoleny aplikace s následujícími typy hazardních produktů: • Sportovní sázení (pouze koňské dostihy, závody motorových člunů, cyklistické a motocyklové závody a fotbalové loterie pořádané státními provozovateli) • Loterie (pouze státní provozovatelé)

Mexiko

Souhrn	Podrobnosti
Povoleno s omezeními	S ohledem na výše uvedené požadavky na aplikace a licencování jsou povoleny aplikace s následujícími typy hazardních produktů: • Internetové kasino • Sportovní sázení • Loterie • Denní fantasy sporty

Nový Zéland

Souhrn	Podrobnosti
Povoleno s omezeními	S ohledem na výše uvedené požadavky na aplikace a licencování jsou povoleny aplikace s následujícími typy hazardních produktů: • Sportovní sázení (pouze státní provozovatelé) • Loterie (pouze státní provozovatelé)

Norsko

Souhrn	Podrobnosti
Povoleno s omezeními	S ohledem na výše uvedené požadavky na aplikace a licencování jsou povoleny aplikace s následujícími typy hazardních produktů: • Internetové kasino • Sportovní sázení • Loterie

Rumunsko

Souhrn	Podrobnosti
Povoleno s omezeními	S ohledem na výše uvedené požadavky na aplikace a licencování jsou povoleny aplikace s následujícími typy hazardních produktů: • Internetové kasino • Sportovní sázení • Loterie (pouze státní provozovatelé)

Španělsko

Souhrn	Podrobnosti
--------	-------------

Souhrn	Podrobnosti
Povoleno s omezeními	S ohledem na výše uvedené požadavky na aplikace a licencování jsou povoleny aplikace s následujícími typy hazardních produktů: • Online kasinové hry • Sportovní sázení • Loterie (pouze státní provozovatelé) • Denní fantasy sporty

Švédsko

Souhrn	Podrobnosti
Povoleno s omezeními	S ohledem na výše uvedené požadavky na aplikace a licencování jsou povoleny aplikace s následujícími typy hazardních produktů: • Online kasinové hry • Sportovní sázení • Loterie (pouze státní provozovatelé)

Spojené království

Souhrn	Podrobnosti
Povoleno s omezeními	S ohledem na výše uvedené požadavky na aplikace a licencování jsou povoleny aplikace s následujícími typy hazardních produktů: • Online kasinové hry • Sportovní sázení • Loterie • Denní fantasy sporty

USA

Souhrn	Podrobnosti
Povoleno s omezeními	S ohledem na výše uvedené požadavky na aplikace a licencování jsou povoleny aplikace s následujícími typy hazardních produktů: • Online kasinové hry (povolené ve státech Delaware, Nevada) (pouze poker), New Jersey a Pensylvánie) • Sportovní sázení (povolené ve státech Colorado, District of Columbia (pouze státní provozovatelé), Illinois, Indiana, Iowa, Montana (pouze státní provozovatelé), Nevada, New Hampshire, New Jersey, Oregon (pouze státní provozovatelé), Pensylvánie, Rhode Island, Tennessee a Západní Virginie) • Loterie (pouze státní provozovatelé nebo spříznění smluvní provozovatelé ve státech Georgia, Illinois, Kentucky, Maine, Michigan, New Hampshire, New York, Severní Karolína, Pensylvánie, Rhode Island a Virginie) • V závislosti na státu mohou být v USA denní fantasy sporty regulovány jako hazardní hry a veškeré aplikace pro denní fantasy sporty publikované v USA podléhají níže uvedeným požadavkům na aplikace pro denní fantasy sporty (DFS).

Způsobilé aplikace musí splňovat následující požadavky:

- Aby vývojář mohl distribuovat aplikaci ve službě Play, musí úspěšně [projít procesem žádosti](#).
- Aplikace musí splňovat všechny příslušné právní předpisy a oborové standardy ve všech zemích, kde je distribuována.
- Vývojář musí mít platnou licenci k provozování hazardních her ve všech zemích a oblastech, kde je aplikace distribuována.
- Vývojář nesmí nabízet typ hazardního produktu, který překračuje rozsah licence k provozování hazardních her.

- Aplikace musí zabraňovat používání nezletilým uživatelům.
- Aplikace musí znemožňovat přístup a použití v zemích, státech/teritoriích nebo zeměpisných oblastech, 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 službu Fakturace 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.

Další hry, soutěže a turnaje se skutečnými penězi

U všech ostatních aplikací, které nesplňují výše uvedené požadavky na způsobilost hazardních aplikací, nepovolujeme obsah či služby, které uživatelům umožňují sázet nebo se jinak podílet pomocí reálných peněz (včetně položek v aplikaci, které lze kupovat za peníze), aby získali cenu ve skutečné peněžní hodnotě. Patří mezi ně mimo jiné internetová kasina, sportovní sázení, loterie a hry, které přijímají peníze a nabízejí ceny v podobě hotovosti nebo jiné reálné hodnoty (s výjimkou programů povolených v rámci níže popsanych požadavků na věrnostní programy s hazardními prvky).

Příklady porušení zásad

- Hry, které přijímají peníze výměnou za příležitost k získání fyzické nebo peněžní ceny.
- Aplikace s navigačními prvky nebo funkcemi (jako jsou položky nabídky, karty, tlačítka, [zobrazení WebView](#) apod.), které vybízejí k sázení nebo k účasti ve hrách, soutěžích nebo turnajích s reálnými penězi, např. aplikace, které uživatele vyzývají stylem „VSAĎTE SI!“, „ZAREGISTRUJTE SE!“ nebo „SOUTĚŽTE!“ a zvou do turnaje s šancí na peněžní výhru.
- Aplikace, které přijímají nebo spravují sázky, měny v aplikaci, výhry nebo vklady, jejichž prostřednictvím lze získat nebo hrát o získání fyzické nebo peněžní ceny.

Věrnostní programy s herními prvky

Pokud to právní předpisy povolují a na příslušný případ se nevztahují další požadavky na licencování hazardu nebo her, povolujeme věrnostní programy, které odměňují uživatele cenami s reálnou hodnotou nebo ekvivalentní peněžní hodnotou, pokud splňují následující požadavky Obchodu Play na způsobilost:

Všechny aplikace (herní i neherní):

- Benefity, výhody nebo odměny ve věrnostním programu musí být jasně uvedeny jako doplňkové a musí být podmíněny oprávněnou peněžní transakcí v rámci aplikace (příčemž příslušná peněžní transakce musí být skutečná samostatná transakce za účelem poskytnutí zboží nebo služeb nezávisle na věrnostním programu) a nesmí být podmíněna nákupem ani být spojena s jakýmkoli způsobem výměny, který by jinak porušoval zásady her, soutěží a hazardních her se skutečnými penězi.
- Například žádná část oprávněné peněžní transakce nesmí představovat poplatek nebo sázku na účast ve věrnostním programu a oprávněná peněžní transakce nesmí vést k nákupu zboží nebo služeb nad rámec obvyklé ceny.

Herní aplikace:

- Věrnostní body nebo odměny lze získat a uplatnit pouze na základě pevně stanoveného ukazatele, který je jasně uveden v aplikaci a také ve veřejně dostupných oficiálních pravidlech programu. Na získání výhod nebo hodnoty k uplatnění se **nesmí** sázet a nesmí být uděleno ani umocněno na základě výkonu ve hře nebo výsledků vzniklých vlivem náhody.

Neherní aplikace:

- Věrnostní body nebo odměny mohou být spojeny se soutěží nebo výsledky vzniklými vlivem náhody, pokud splňují níže uvedené požadavky. Věrnostní programy s benefity, výhodami nebo cenami spojenými s oprávněnou peněžní transakcí musí splnit tyto požadavky:
 - V aplikaci musí být zveřejněna oficiální pravidla programu.
 - U programů se systémem odměny založeným na proměnné nebo náhodě: V oficiálních pravidlech programu je třeba uvést 1) metodu výpočtu pravděpodobnosti výhry (u programů s fixní pravděpodobností) a 2) metodu výběru výherce (u ostatních programů).
 - V oficiálních pravidlech programu, který nabízí losování, sázky nebo jiný podobný styl propagačních akcí, je třeba uvést pevný počet výherců, pevný termín pro účast a datum přidělení výhry v rámci každé propagační akce.
 - Je třeba zdokumentovat viditelně v aplikaci a v oficiálních pravidlech programu pevný poměr připisování věrnostních bodů či odměn a jejich získávání.

Typ aplikace s věrnostním programem	Věrnostní program s herními prvky a proměnlivými odměnami	Věrnostní odměny na základě pevně stanoveného ukazatele/plánu	Povinnost uvést smluvní podmínky věrnostního programu	Smluvní podmínky musí udávat pravděpodobnost výhry ve věrnostním programu na základě náhody nebo metodu výběru výherce
Herní	Nepovoleno	Povoleno	Vyžadováno	Nevztahuje se (herní aplikace nemají povoleno využívat ve věrnostních programech prvky založené na náhodě)
Neherní	Povoleno	Povoleno	Vyžadováno	Vyžadováno

Reklamy na hazardní hry nebo aplikace distribuované ve službě Play, které obsahují hry, turnaje a soutěže se skutečnými penězi

Aplikace obsahující reklamy, které propagují hazardní hry, hry se skutečnými penězi, soutěže a turnaje, povolujeme pouze v případě, že jsou splněny následující požadavky:

1. Aplikace a reklama (včetně inzerentů) musí splňovat všechny příslušné zákony a oborové standardy ve všech oblastech, kde se reklama zobrazuje.
2. Reklama musí splňovat příslušné místní licenční podmínky pro všechny propagované produkty a služby související s hazardními hrami.
3. Aplikace nesmí reklamu na hazardní hru zobrazovat osobám, o kterých je známo, že jsou mladší 18 let.
4. Aplikace nesmí být zařazena do programu Pro celou rodinu.
5. Aplikace nesmí cílit na osoby mladší 18 let.
6. Reklama na hazardní aplikaci (jak je definováno výše) musí na vstupní stránce, v záznamu inzerované aplikace nebo v samotné aplikaci jasně zobrazovat informaci o zodpovědném hraní hazardních her.
7. Aplikace nesmí poskytovat simulace obsahu týkajícího se hazardních her (např. aplikace pro kasinové hry pro zábavu, aplikace s virtuálními hracími automaty apod.).
8. Aplikace nesmí poskytovat funkce podporující hazard nebo hry, loterie či turnaje se skutečnými penězi ani doprovodné funkce (např. funkce, které pomáhají se sázením, platbami, sledováním sportovních výsledků/tipů/výkonů nebo správou prostředků v hazardních hrách).
9. Obsah aplikace nesmí propagovat ani uživatele přesměrovávat na služby spojené s hazardem nebo hrami, loteriemi či turnaji se skutečnými penězi.

Reklamy na hazardní hry nebo hry, loterie a soutěže se skutečnými penězi mohou obsahovat pouze aplikace, které splňují všechny požadavky uvedené v této sekci. Přijaté hazardní aplikace (definovány výše) nebo přijaté aplikace pro denní fantasy sporty (definovány níže), které splňují výše uvedené požadavky 1–6, mohou obsahovat reklamy na hazardní hry nebo hry, loterie a soutěže se skutečnými penězi.

Příklady porušení zásad

- Aplikace navržena pro nezletilé, která obsahuje reklamu na služby hazardního hraní.
- Simulovaná kasinová hra, která propaguje nebo přesměrovává uživatele na kasinové hry se skutečnými penězi.
- Speciální aplikace pro sledování sportovních výsledků a tipů, která obsahuje integrované reklamy na stránky se sportovním sázením.
- Aplikace obsahující reklamy na hazardní hry, které porušují naše zásady týkající se (např. reklamy, které se uživatelům v aplikaci zobrazují jako tlačítka, ikony nebo jiné interaktivní prvky).

Aplikace pro denní fantasy sporty (DFS)

Aplikace pro denní fantasy sporty (DFS) povolujeme pouze v případě, že jsou v souladu s místními právními předpisy a splňují následující požadavky:

- Aplikace je buď 1) distribuována výhradně ve Spojených státech, nebo 2) splňuje výše uvedené požadavky na hazardní aplikace.
- Aby vývojář mohl distribuovat aplikaci ve službě Play, musí úspěšně dokončit [proces žádosti pro DFS](#) a musí být přijat.
- Aplikace musí splňovat všechny příslušné zákony a oborové standardy každé země, kde je distribuována.

- Aplikace musí zabraňovat nezletilým uživatelům v sázení a provádění peněžních transakcí v aplikaci.
- Aplikace na Google Play NESMÍ být k dispozici ke koupi jako placená a nesmí ani používat službu Fakturace 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 případě distribuce v USA je třeba splňovat i následující požadavky:

- 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 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.

Nezákonné činnosti

Nepovolujeme aplikace, které zprostředkovávají nebo propagují nezákonné činnosti.

Příklady běžných porušení zásad:

- 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.

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.
- Ve smluvních podmínkách nebo v zásadách pro uživatele aplikace musejí definovat nevhodný obsah a chování (v souladu s programovými zásadami pro vývojáře služby Play) a zakázat je.
- 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 případě aplikací ke streamování přímých přenosů musí být nežádoucí obsah vytvářený uživateli odstraněn, co nejdříve je to přiměřeně možné.
 - V případě aplikací s rozšířenou realitou (RR) musí moderování obsahu vytvářeného uživateli (včetně systému přehledů v aplikaci) brát v potaz jak uživatelé vytvářejí nevhodný obsah s RR (například sexuálně explicitní obrázky v RR), tak i citlivou polohu ukotvení v RR (např. obsah v RR ukotvený v zakázané oblasti, například na vojenské základně nebo na soukromém majetku, kde by ukotvení v RR mohlo majiteli způsobit problémy).
- V aplikaci musí být k dispozici uživatelsky přívětivý systém k nahlášení nežádoucího obsahu vytvářeného uživateli.
- Musejí odebírat 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.

Příklady běžných porušení zásad:

- Propagace sexuálně explicitního obsahu vytvářeného uživateli, včetně implementace nebo povolení placených funkcí, které uživatele motivují ke sdílení nevhodného obsahu.
- Aplikace s obsahem vytvářeným uživateli, které neobsahují dostatečná opatření proti vyhrožování, 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 doplncích naleznete na webu www.legitscript.com.

Duševní vlastnictví

Když vývojáři kopírují cizí práci nebo bez dovolení používají cizí dílo, mohou tím poškodit majitele tohoto díla. Neuchylujte se k neférovému využívání cizí práce.

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). Nepovolujeme ani 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 paděláních](#).

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 v 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 nedošlo k zamítnutí aplikace 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.

Zde je několik případů používání obsahu chráněného autorskými právy bez povolení nebo právně opodstatněného důvodu:

- 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 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.

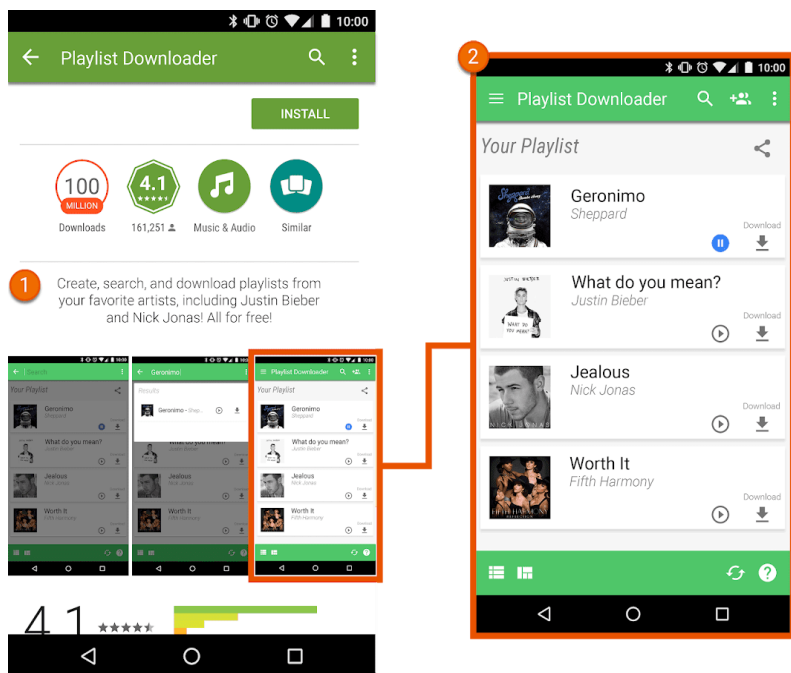
- Aplikace se zvukovou klávesnicí, která přehrává zvukové klipy z obsahu chráněného autorskými právy.
- Úplné reprodukce nebo překlady knih, které se nenacházejí ve veřejném vlastnictví.

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.

Příklady běžných porušení zásad:

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

Ochrana soukromí, ochrana před podvody a zabránění zneužití zařízení

Snažíme se chránit soukromí uživatelů a poskytovat jim bezpečné prostředí. Aplikace, které jsou klamavé, škodlivé, nebo mají za cíl zneužít síť, zařízení nebo osobních údajů, jsou přísně zakázány.

Uživatelská data

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 údaje shromažďuje, používá a sdílí, a vy je smíte 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, údaje 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 jakým typům třetích stran 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 nemuseli přiměřeně očekávat, že k poskytování či vylepšování funkcí aplikace, které jsou v souladu se zásadami, budou potřeba jejich osobní nebo citlivé údaje (např. ke shromažďování údajů dochází na pozadí aplikace), máte následující povinnosti:

Aplikace musí obsahovat oznámení o přístupu k údajům, 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 k vyjádření souhlasu uživatele použity zprávy, které se samy zavrou (např. po vypršení časového limitu).

Příklady běžných porušení zásad:

- Aplikace, která na základě výše uvedených zásad ochrany soukromí, zpracování údajů, viditelných oznámení a udělení souhlasu nepovažuje za osobní ani citlivé údaje informace o nainstalovaných aplikacích uživatele.
- Aplikace, která na základě výše uvedených zásad ochrany soukromí, zpracování údajů, viditelných oznámení a udělení souhlasu nepovažuje za osobní ani citlivé údaje telefonní číslo nebo seznam kontaktů uživatele.
- Aplikace, která zaznamenává obsah obrazovky uživatele a se získaným záznamem nezachází jako s osobními či citlivými daty v souladu s těmito zásadami.
- Aplikace, která používá [polohu zařízení](#), aniž by o tom poskytovala úplné informace a získala souhlas v souladu s výše uvedenými požadavky.
- Aplikace, která shromažďuje omezená oprávnění na pozadí aplikace, například za účelem sledování, výzkumu či marketingu, aniž by o tom poskytovala úplné informace a získala souhlas v souladu s výše uvedenými požadavky.

Konkrétní 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 jakými typy třetích stran 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.

Oprávnění

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 navíc v dokumentaci pro vývojáře označena štítkem **Nebezpečné**, **Zvláštní** nebo **Podpis** 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 byly příslušné údaje získány. Údaje 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 údajů 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 citlivé údaje o uživateli a vztahují se na ně zásady uvedené v sekci [Osobní a citlivé údaje](#) a následující omezení:

Omezené oprávnění	Požadavek
Manifest aplikace vyžaduje oprávnění ze skupiny Hovory (např. <code>READ_CALL_LOG</code> , <code>WRITE_CALL_LOG</code> , <code>PROCESS_OUTGOING_CALLS</code>)	Musí být v zařízení aktivně zaregistrován jako výchozí obslužný nástroj typu Telefon nebo Asistence.
Manifest aplikace vyžaduje oprávnění ze skupiny SMS (např. <code>READ_SMS</code> , <code>SEND_SMS</code> , <code>WRITE_SMS</code> , <code>RECEIVE_SMS</code> , <code>RECEIVE_WAP_PUSH</code> , <code>RECEIVE_MMS</code>).	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 nesmí. 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. Základní funkčnost je hlavním účelem aplikace. Může zahrnovat sadu základních funkcí, které musí být všechny jasně zdokumentovány a propagovány v popisu aplikace. Bez základní funkčnosti 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

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](#).

Oprávnění k přístupu ke všem souborům

Soubory a atributy adresáře na uživatelově zařízení jsou považovány za osobní a citlivé údaje, na které se vztahují zásady uvedené v sekci [Osobní a citlivé údaje](#) a následující požadavky:

- Aplikace by měly žádat pouze o takový přístup k úložišti zařízení, který je zásadně důležitý pro funkčnost aplikace. Nesmí žádat o přístup k úložišti zařízení jménem třetí strany za účelem, který nesouvisí se zásadní funkčností aplikace

vůči uživateli.

- Zařízení Android s verzí R (Android 11, úroveň rozhraní API 30) nebo novější budou vyžadovat oprávnění [MANAGE_EXTERNAL_STORAGE](#), aby mohla spravovat přístup ve sdíleném úložišti. Všechny aplikace, které cílí na R a vyžadují široký přístup ke sdílenému úložišti (přístup ke všem souborům), musí před publikováním úspěšně projít příslušnou kontrolou přístupu. Aplikace, u kterých je toto oprávnění povoleno, musejí v aplikaci uživatele jasně požádat, aby v nastavení Zvláštní přístup aplikací povolili možnost Přístup ke všem souborům. Další informace o požadavcích na R najdete v tomto [článku nápovědy](#).

Zneužívání zařízení a sítí

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 sítí autorizovaného operátora), popř. které je narušují, poškozují nebo v nich získávají neoprávněný přístup.

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

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).

Nepovolujeme kód, který vnáší chyby zabezpečení nebo je zneužívá. Další informace o nejnovějších bezpečnostních problémech, které byly vývojářům nahlášeny, naleznete v [Programu zvyšování zabezpečení aplikací](#).

Příklady běžných porušení zásad:

- 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 nesplňují podmínky pro [zařazení na seznam povolených aplikací](#) a pokoušejí se obejít [systémové řízení spotřeby](#).
- Aplikace, které zprostředkovávají služby proxy třetím stranám, tak mohou činit pouze v případě, že se jedná o primární a pro uživatele jasně viditelný účel aplikace.
- Aplikace nebo kód třetí strany (např. sady SDK, které stahují spustitelný kód (jako jsou soubory DEX nebo nativní kód) z jiného zdroje než Google Play.
- Aplikace, které bez předchozího souhlasu uživatele do zařízení instalují jiné aplikace.
- Aplikace, které odkazují na škodlivý software, popř. zprostředkovávají jeho distribuci nebo instalaci.

Klamavé chování

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/videoa funkcí. 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 vrátit zpět.

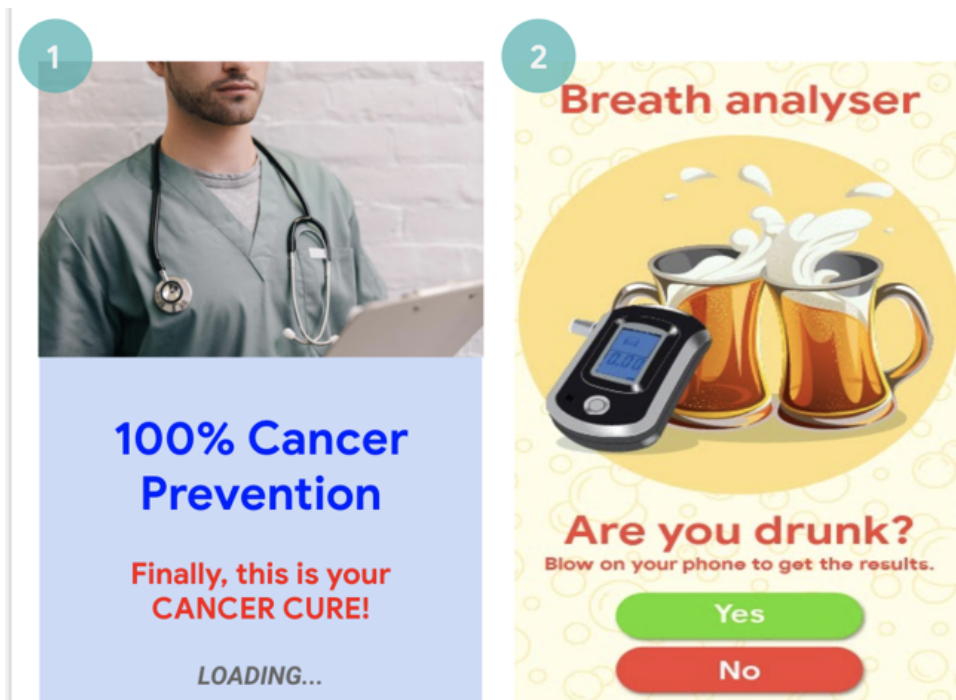
Zavádějící tvrzení

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

Příklady běžných porušení zásad:

- 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 (např. aplikace sloužící jako odpuzovač hmyzu), i když jsou představovány jako žertovné, falešné, vtipné apod.
- Aplikace, které jsou zařazeny do nesprávné kategorie (například hodnocení aplikace nebo kategorie aplikace).
- 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.
- Aplikace, které nepravdivě uvádějí, že jsou oficiální aplikací zavedeného subjektu. Bez potřebných oprávnění nebo práv nelze používat například názvy jako Oficiální aplikace Karla Gotta.



- (1) Aplikace obsahuje zavádějící lékařské údaje nebo údaje týkající se zdraví (léčba rakoviny)
 (2) Aplikace tvrdí, že obsahuje funkce, které nelze implementovat (použití telefonu k analýze dechové zkoušky)

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.

Dodatečné zdroje aplikací (například herní podklady) je dovoleno stahovat jen v případě, že jsou k používání aplikace nezbytné. Stahované zdroje musí 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.

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

Příklady běžných porušení zásad:

- Aplikace, které 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, jejichž různé základní funkce jsou založeny na zeměpisné poloze uživatele, parametrech zařízení nebo na jiných údajích závislých na uživateli, aniž by byl uživatel o těchto rozdílech informován přímo v záznamu v obchodu.
- Aplikace, jejichž jednotlivé verze se výrazně mění, aniž by na to byl uživatel upozorněn (např. [v části Novinky](#)) a aniž by byl aktualizován záznam v obchodu.
- Aplikace, které se při kontrole pokoušejí upravovat nebo obfuskovat.
- Aplikace, které stahují obsah ze sítě CDN, aniž by uživatele před zahájením stahování informovaly o velikosti stahovaného obsahu a požádaly o svolení.

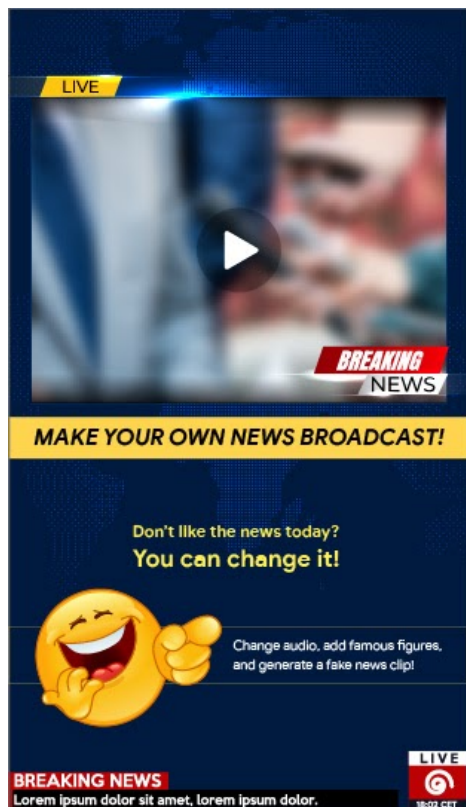
Manipulace s médii

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.

Příklady běžných porušení zásad:

- 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.



(1) Tato aplikace nabízí funkce pro úpravu mediálních klipů, které slouží k napodobení zpravodajského vysílání, a bez vodoznaku do videoklipu přidává slavné nebo veřejně činné osobnosti.

Předstírání identity

Nepovolujeme aplikace ani účty vývojářů, které vykazují některé z následujících vlastností:

- Předstírají identitu jiné osoby nebo organizace, případně skrývají či nepravdivě uvádějí svého vlastníka nebo primární účel.
- Zapojují se 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.
- V koordinaci s jinými aplikacemi, weby, vývojáři nebo jinými účty skrývají nebo nepravdivě uvádějí identitu vývojáře či aplikace nebo jiné důležité podrobnosti, pokud obsah aplikace souvisí s politikou, sociálními problémy nebo záležitostmi veřejného zájmu.

Malware

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.

Malware

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.

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 bude moci útočník získat přístup k napadenému zařízení 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 zároveň se snaží 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 může služba Google Play Protect 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 zatažení SMS zpráv od mobilního operátora, které uživatele informují o platbách nebo potvrzují předplatné.

Podvod s hovorem

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

Podvod s poplatkem

Kód, který uživatele podvodem přiměje k předplacení nebo zakoupení obsahu prostřednictvím vyúčtování za mobilní služby.

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 uživatele 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.

Stalkerware

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

Stalkerwarové aplikace obvykle přenášejí data jiné straně, než je poskytovatel potenciálně škodlivé aplikace.

Přijatelné typy těchto aplikací mohou používat rodiče ke sledování dětí. Pomocí těchto aplikací však nelze sledovat osobu (například manžela nebo manželku) bez jejího vědomí nebo svolení, pokud během přenosu dat není zobrazeno trvalé oznámení.

Jediné aplikace s funkcemi sledování a hlášení, které lze v Obchodě 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.

Aplikace distribuované v Obchodě Play, které v zařízení sledují chování uživatele, nejsou považovány za stalkerware, pokud splňují alespoň následující požadavky:

- Aplikace se nesmějí prezentovat jako řešení určené ke špehování nebo skrytému sledování.
- Aplikace nesmějí skrývat ani maskovat sledovací funkce ani o nich uživatelům poskytovat zavádějící informace.
- Aplikace uživatelům musejí zobrazovat trvalé oznámení a jedinečnou ikonu, které aplikaci jasně identifikují.
- Aplikace a záznamy aplikací na Google Play nesmějí žádným způsobem umožňovat aktivaci nebo použití funkcí, které porušují tyto podmínky (například prostřednictvím propojení se soubory APK hostovanými mimo Google Play, které nesplňují tyto zásady).
- 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.

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 projevit například odesláním 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 stáhl 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 kradе 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 nespouští 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 budou například 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 malware. 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 my nemáme důvod se domnívat, 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.

Nevyžádaný software pro mobilní zařízení

Tyto zásady vycházejí ze zásad společnosti Google ohledně nevyžádaného softwaru a popisují pravidla pro [ekosystém Android](#) a Obchod Google Play. Software, který tato pravidla porušuje, je pro uživatele potenciálně škodlivý, a proto se budeme snažit před ním uživatele chránit.

Nevyžádaný software pro mobilní zařízení

Ve společnosti Google věříme, že když se zaměříme na uživatele, vše ostatní přijde samo. V našich [pravidlech pro software](#) a v [zásadách ohledně nevyžádaného softwaru](#) poskytujeme obecná doporučení týkající se softwaru, který vytváří skvělý uživatelský dojem. Tyto zásady vycházejí ze zásad společnosti Google ohledně nevyžádaného softwaru a popisují pravidla pro [ekosystém Android](#) a Obchod Google Play. Software, který tato pravidla porušuje, je pro uživatele potenciálně škodlivý, a proto se budeme snažit před ním uživatele chránit.

Jak je v [zásadách ohledně nevyžádaného softwaru](#) uvedeno, zjistili jsme, že nežádoucí software většinou vykazuje jednu nebo několik ze základních charakteristik:

- Je klamavý a slibuje hodnotu, kterou následně neposkytuje.
- Snaží se uživatele klamavě přimět k instalaci nebo se nainstalovat současně s instalací jiného programu.
- Neinformuje uživatele o svých hlavních a významných funkcích.
- Nečekaným způsobem ovlivňuje systém uživatele.
- Bez vědomí uživatele shromažďuje nebo odesílá soukromé informace.

- Shromažďuje nebo přenáší soukromé informace, aniž by používal zabezpečení (například přenos přes protokol HTTPS).
- Je přibalen k jinému softwaru a uživatel o jeho přítomnosti není informován.

V mobilních zařízeních se softwarový kód nachází ve formě aplikace, binárního kódu, úprav aplikačního rámce apod. Na obranu před softwarem, který poškozuje softwarový ekosystém nebo narušuje uživatelský dojem, podnikneme příslušná opatření.

Níže vycházíme ze zásad ohledně nevyžádaného softwaru, jejichž použití rozšiřujeme i na mobilní zařízení. V souladu s těmito zásadami budeme zlepšovat i zásady ohledně nevyžádaného softwaru pro mobilní zařízení, abychom předcházeli novým typům zneužití.

Transparentní chování a jasné údaje o zveřejňování

Veškerý kód by měl plnit sliby, které uživateli dal. Aplikace by měly poskytovat všechny avizované funkce. Aplikace by uživatele neměly klamat.

- Aplikace by měly mít jasně stanovené funkce a cíle.
- Jasně a zřetelně uživateli vysvětlíte, jaké změny v systému aplikace provede. Umožněte uživatelům při instalaci zkontrolovat a schválit všechny důležité možnosti a změny.
- Software by uživateli neměl prezentovat klamavá sdělení o jeho zařízení (například tvrzením, že systém je ohrožen kritickou chybou zabezpečení nebo že je zavírován).
- Nepoužívejte neplatnou aktivitu určenou ke zvyšování návštěvnosti reklam nebo ke konverzím.
- Nepovolujeme aplikace, které uživatele klamou tím, že se vydávají za někoho jiného (např. za jiného vývojáře, společnost, subjekt apod.) nebo za jinou aplikaci. Nenaznačujte, že vaše aplikace s někým souvisí nebo že je někým schválena, pokud tomu tak není.

Příklady porušení zásad:

- Inzertní podvody
- Předstírání jiné identity

Chraňte údaje o uživateli

Jasně a transparentně vysvětlíte způsob používání, shromažďování a sdílení osobních a citlivých údajů o uživateli a přístup k nim. Použití údajů o uživateli musí být pokud možno v souladu se všemi příslušnými zásadami ohledně údajů o uživateli, a je třeba podniknout veškerá opatření k jejich ochraně.

- Dejte uživatelům možnost vyjádřit souhlas se shromažďováním údajů ještě předtím, než tyto údaje začnete shromažďovat a odesílat ze zařízení. Týká se to údajů o účtech třetích stran, e-mailů, telefonních čísel, nainstalovaných aplikací, souborů, polohy a dalších osobních a citlivých údajů, jejichž shromažďování by uživatel nemusel očekávat.
- S osobními a citlivými údaji o uživateli, které shromažďujete, je třeba nakládat zabezpečeným způsobem a přenášet je s využitím moderního šifrování (např. pomocí protokolu HTTPS).
- Software (včetně mobilních aplikací) smí osobní a citlivé údaje o uživateli na servery přenášet pouze v případě, že je tento přenos spojen s funkcí aplikace.

Příklady porušení zásad:

- Shromažďování dat (srov. [Spyware](#))
- Zneužití omezených oprávnění

Příklady zásad ohledně údajů o uživateli:

- [Zásady ohledně údajů o uživateli služby Google Play](#)
- [Požadavky na GMS – Zásady ohledně údajů o uživateli](#)
- [Zásady ohledně údajů o uživateli služby Google API](#)

Neohrožujte mobilní prostředí

Uživatelský dojem by měl být jasný, snadno srozumitelný a měl by být založen na výběru z jasných možností ze strany uživatele. Uživatel by měl dostat jasnou hodnotovou nabídku a inzerovaný či očekávaný uživatelský dojem by neměl být ničím rušen.

- Nepoužívejte reklamy, které se uživatelům zobrazují neočekávaným způsobem (například poškozováním nebo narušováním funkcí zařízení, zobrazováním mimo prostředí aplikace) a nelze je snadno zavřít. Také používejte vhodný souhlas a atribuci.
- Aplikace nesmí zasahovat do jiných aplikací ani narušovat použitelnost zařízení.
- V rámci možností by měla být jasně uvedena možnost odinstalování.
- Mobilní software nesmí napodobovat výzvy operačního systému zařízení ani jiných aplikací. Nepotlačujte upozornění jiných aplikací ani operačního systému, zvláště taková, která uživatele informují o změnách v operačním systému.

Příklady porušení zásad:

- Rušivé reklamy
- Neoprávněné používání nebo nápodoba funkcí systému

Inzertní podvody

Inzertní podvody jsou přísně zakázány. Interakce s reklamou, generované za účelem oklamat reklamní síť, aby se domnívala, že provoz pochází od autentických uživatelů, je inzertním podvodem, který je formou [neplatného provozu](#). Inzertní podvod může být vedlejším produktem toho, když vývojáři implementují reklamy nepovoleným způsobem, např. zobrazují skryté reklamy nebo reklamy s automatickým proklikem, upravují informace nebo jinak využívají strojové akce (roboti) nebo lidskou aktivitu k produkci neplatného reklamního provozu. Neplatný provoz a podvody spojené s reklamami jsou pro inzery, vývojáře a uživatele škodlivé a vedou k dlouhodobé ztrátě důvěry v ekosystém mobilních reklam.

Příklady běžných porušení zásad:

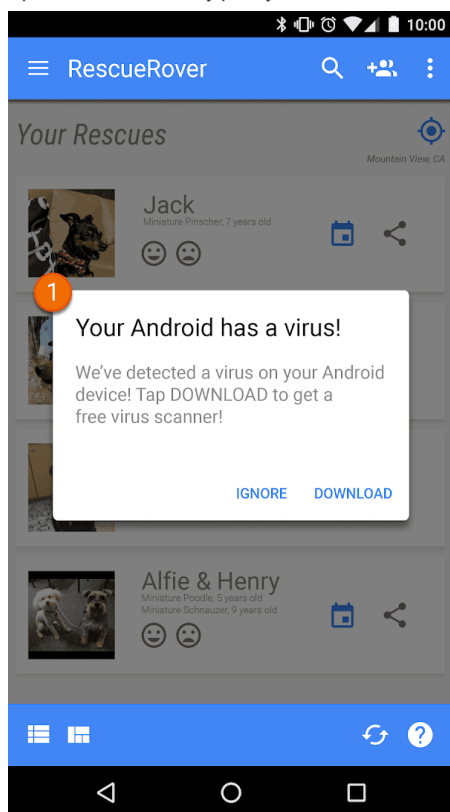
- Aplikace zobrazující reklamy, které nejsou pro uživatele viditelné.
- Aplikace, která bez záměru uživatele automaticky generuje kliknutí na reklamy nebo která generuje ekvivalentní síťový provoz za účelem podvodného přiřazení kreditů za kliknutí.
- Aplikace odesílající falešná kliknutí na atribuci instalace, aby dostala zaplacení za instalace, které nepocházejí ze sítě odesílatele.
- Aplikace zobrazující reklamu, když se uživatel nenachází v rozhraní aplikace.
- Nepravdivá tvrzení reklamní plochy aplikace, např. aplikace, která s reklamními sítěmi komunikuje, jako by byla spuštěna na zařízení iOS, přestože je ve skutečnosti spuštěna na zařízení Android, případně aplikace, která nepravdivě uvádí název monetizovaného balíčku.

Neoprávněné používání nebo nápodoba funkcí systému

Nepovolujeme aplikace ani reklamy, 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).

Příklady běžných porušení zásad:

- 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 týkající se reklam naleznete v [zásadách inzerce](#).

Předstírání jiné identity

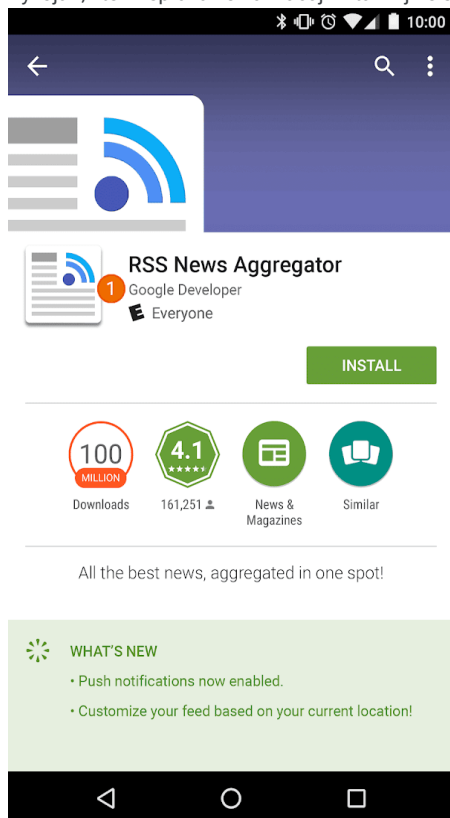
Když vývojáři předstírají jinou identitu nebo své aplikace vydávají za cizí, klamou uživatele a poškozují celou komunitu vývojářů. Aplikace, které předstíráním jiné identity klamou uživatele, jsou zakázány.

Předstírání jiné identity

Nepovolujeme aplikace, které uživatele klamou tím, že se vydávají za někoho jiného (např. za jiného vývojáře, společnost, subjekt apod.) nebo za jinou aplikaci. Nenaznačujte, že vaše aplikace s někým souvisí nebo že je někým schválena, pokud tomu tak není. Nepoužívejte ikony aplikací, popisy, názvy ani prvky aplikace, které by mohly uživatele mást ohledně vztahu vaší aplikace k jiné osobě nebo aplikaci.

Příklady běžných porušení zásad:

- Vývojáři, kteří nepravdivě naznačují vztah k jiné společnosti nebo vývojáři:



① Jméno vývojáře uvedené u této aplikace naznačuje oficiální vztah ke společnosti Google, přestože 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

Zpeněžení a reklamy

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. Vzhledem k tomu, že chceme zajistit co nejlepší uživatelský dojem, vyžadujeme, abyste dodržovali následující zásady.

Platby

1. Vývojáři, kteří účtují poplatky za aplikace a obsah stahovaný z Google Play, musí používat fakturační systém Google Play.
2. Aplikace distribuované na Google Play musí jako platební metodu používat fakturační systém Google Play, pokud za účelem získání přístupu k funkcím nebo službám (včetně funkcí aplikace, digitálního obsahu nebo zboží) vyžadují nebo přijímají platbu.
 - a. Mezi funkce aplikací nebo služby, které vyžadují použití fakturačního systému Google Play, patří mimo jiné i tyto nákupy v aplikaci:
 - položky (například virtuální měny, životy navíc, další herní čas, doplňky, postavy a avatary),
 - předplacené služby (např. fitness, hra, seznamování, vzdělávání, hudba, video nebo jiné služby s předplaceným obsahem),
 - funkce nebo obsah aplikace (např. verze aplikace bez reklam nebo nové funkce, které bezplatná verze nenabízí),
 - cloudový software a služby (například služby úložiště dat, software pro zvýšení firemní produktivity nebo software pro správu financí).
 - b. Fakturační systém služby Google Play nesmí být používán v případech, kdy:
 - je platba primárně určena:
Poznámka: Na některých trzích nabízíme aplikacím, které prodávají fyzické produkty a služby, službu Google Pay. Další informace naleznete na [stránce o službě Google Pay pro vývojáře](#).
 - k nákupu nebo vypůjčení fyzického zboží (například potravinářské zboží, oblečení, domácí potřeby či elektronika),
 - k nákupu fyzicky poskytovaných služeb (například přepravní služby, úklidové služby, letenky, členství v posilovně, dovoz jídla či vstupenky na akce),
 - k platbě účtů kreditní nebo debetní kartou (např. za kabelové a telekomunikační služby),
 - platba zahrnuje platby mezi dvěma smluvními stranami, úhrady online aukcí nebo dary osvobozené od daní,
 - platba je za obsah či služby, které zpřístupňují online hazard, jak je popsáno v sekci [Hazardní aplikace](#) v zásadách pro [hazardní hry, hry a soutěže se skutečnými penězi](#),
 - platba se týká kategorie produktů, která je podle [obsahových zásad centra plateb](#) Google považována za nepřijatelnou.
3. Jiné aplikace než jsou uvedené v části 2(b) nesmí uživatele přesměřovávat na jinou platební metodu než fakturační systém služby Google Play. Tento zákaz zahrnuje přesměrování uživatelů na jiné platební metody mimo jiné těmito způsoby:
 - záznamem aplikace na Google Play,
 - propagací v aplikaci související s prodáváním obsahem,
 - zobrazeními v aplikacích, tlačítky, odkazy, zprávami, reklamami nebo jinými výzvami k akcím,
 - procesy uživatelského rozhraní v aplikaci (například vytváření účtu nebo registrace k němu), které uživatele přesměřovávají z aplikace k jiné platební metodě, než je fakturační systém služby Google Play.
4. Virtuální měny v aplikacích smí být používány pouze v aplikaci nebo hře, ve které byly koupeny.
5. Vývojáři musí uživatele jasně a přesně informovat o podmínkách a cenách aplikace, funkcích v aplikaci a variantách předplatného nabízeného ke koupi. Ceny v aplikaci musí odpovídat cenám ve fakturačním rozhraní služby Play. Pokud v popisu produktu na Google Play informujete o funkcích v aplikaci, které mohou být nějakým dalším způsobem zpoplatněny, musí být ze záznamu aplikace uživatelům jasné, že je přístup k těmto funkcím podmíněn platbou.
6. Aplikace a hry, které umožňují nákupy náhodných virtuálních položek (mimo jiné tzv. loot boxy), musí před nákupem jasně a včasné informovat o pravděpodobnosti získání takových položek.

Předplatná

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

V aplikaci: Nabídka musí být transparentní. To zahrnuje explicitní popis nabídky, včetně ceny předplatného, frekvence fakturačního cyklu a skutečnosti, zda je používání aplikace podmíněno předplatným. Tyto informace se musí zobrazit automaticky, aniž by uživatel prováděl jakoukoli další akci.

Příklady běžných porušení zásad:

- 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).

Get AnalyzeAPP Premium

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

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

Try for \$12.50!

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.

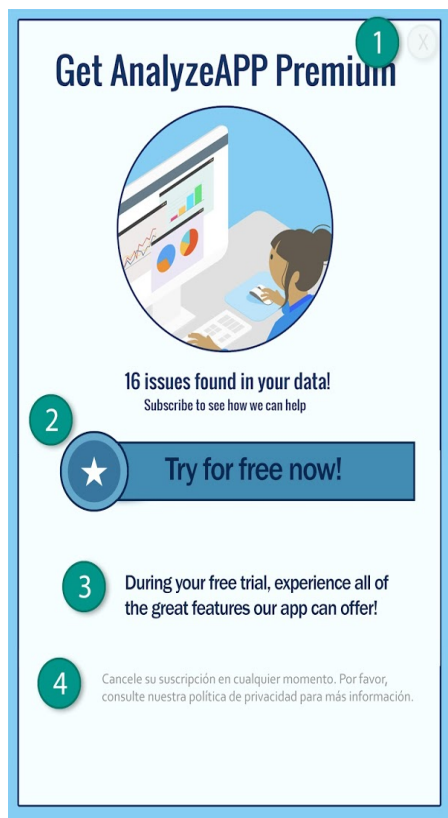
Bezplatná zkušební období a zaváděcí nabídky

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.

Příklady běžných porušení zásad:

- 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 či aplikacích bude srozumitelně uvedeno, jak může uživatel předplatné spravovat či zrušit.

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.

Reklamy

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 musí 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.

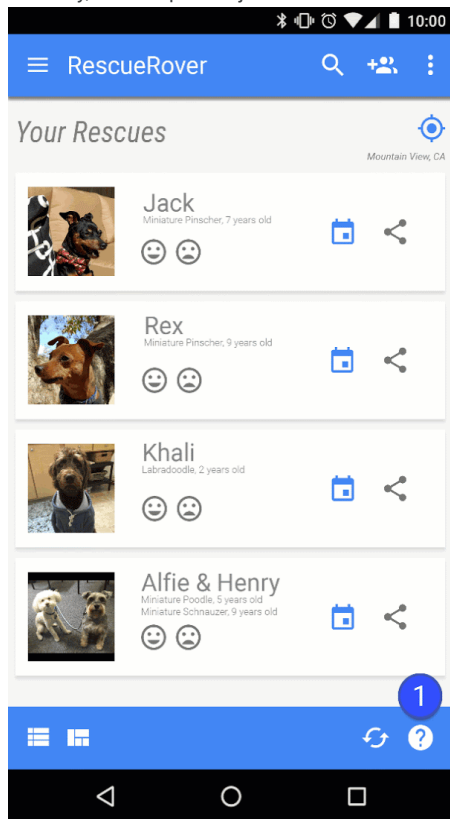
- V souladu s požadavky na [oprávnění pro přístup k poloze](#) je o toto oprávnění dovoleno žádat pouze za účelem implementace aktuálních funkcí nebo služeb aplikace. O toto oprávnění není dovoleno žádat výhradně pro účely zobrazování reklam.

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.

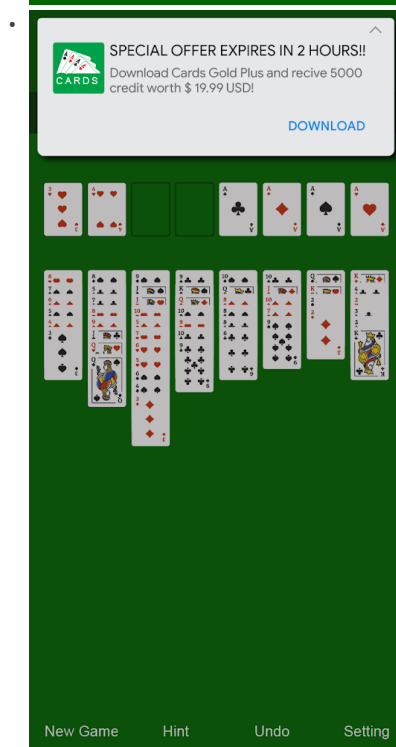
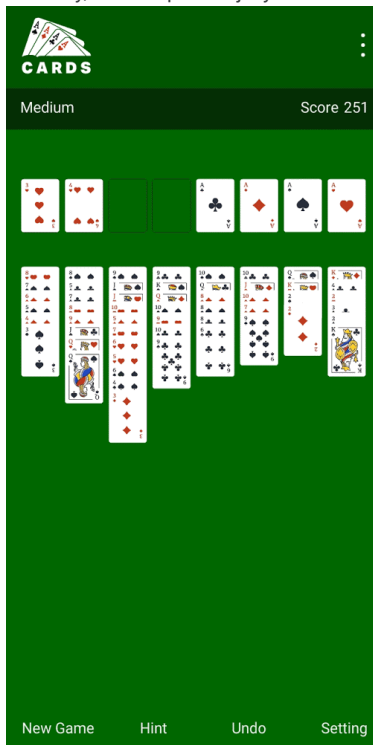
Příklady běžných porušení zásad:

- 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:



Výše uvedené příklady znázorňují reklamy napodobující různá systémová oznámení.

Zpeněžení obrazovky uzamčení

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

Rušivé reklamy

Rušivé reklamy jsou reklamy, které se uživatelům zobrazují neočekávaným způsobem, což může vést k nechtěným kliknutím nebo narušit použitelnost funkcí zařízení.

Aplikace nesmí uživatele nutit, aby dříve, než bude moci aplikaci plně používat, klikal na reklamu nebo odesílal osobní údaje k reklamním účelům. Vsunutá reklama se může zobrazovat pouze v aplikaci, která její zobrazení realizuje. Pokud

aplikace zobrazuje vsunuté nebo jiné reklamy, které narušují běžnou práci s aplikací, musíte uživateli umožnit tyto reklamy snadno zavřít bez jakékoli penalizace.

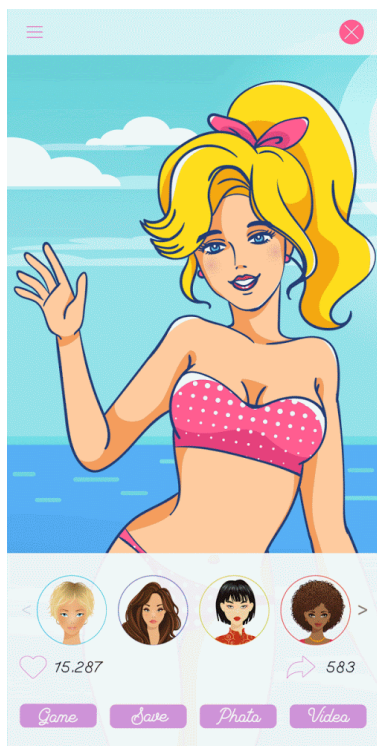
Příklady běžných porušení zásad:

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

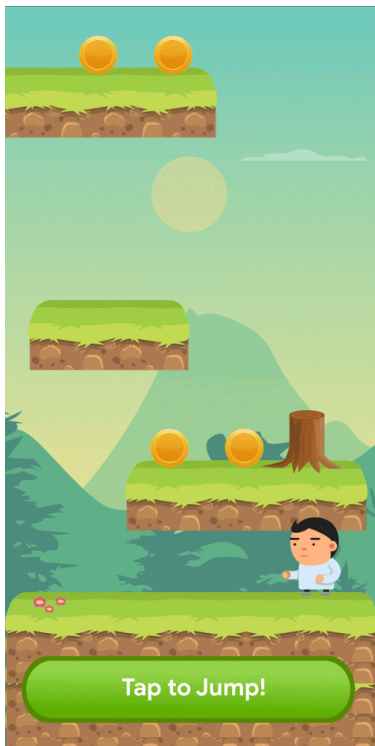


① Tato reklama nemá tlačítko pro zavření.

- Reklamy, které se uživatele snaží přimět kliknout na falešné tlačítko pro zavření nebo které se najednou objeví v částech aplikace, kde uživatel obvykle klepá na jinou funkci.



Reklama, která používá falešné tlačítko pro zavření.



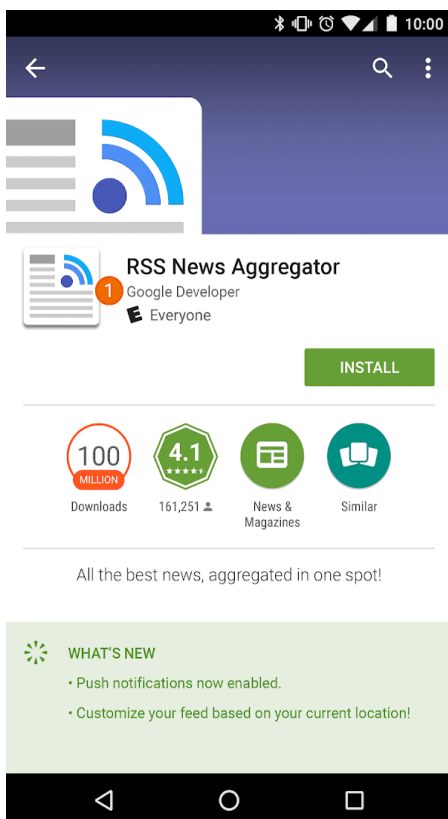
Reklama, která se náhle zobrazí v oblasti, kde uživatel obvykle klepá na jinou funkci aplikace.

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 tlačítek systému a zařízení nebo portů). To zahrnuje překryvné reklamy, funkce doprovodné reklamy i reklamní jednotky v podobě widgetů. Reklamy se mohou zobrazovat pouze v aplikaci, která jejich zobrazení realizuje.

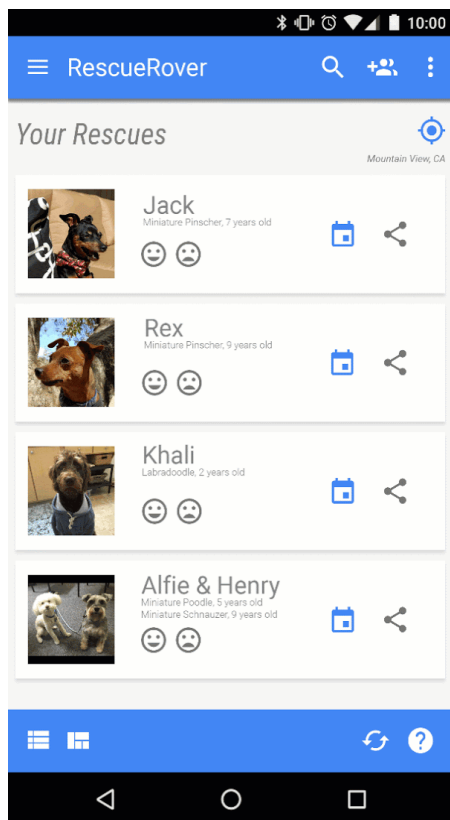
Příklady běžných porušení zásad:

- 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:

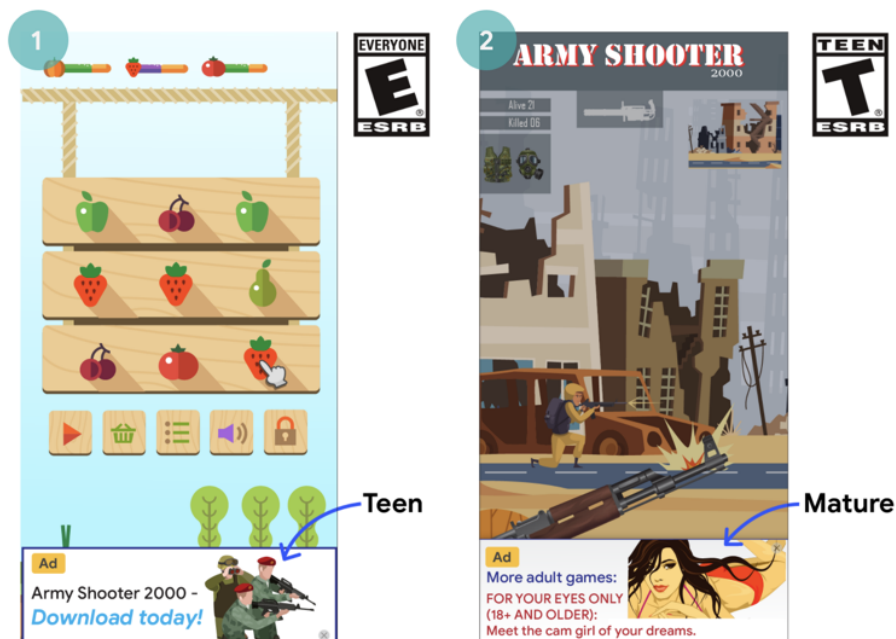


Popis: Uživatel se snaží aplikaci opustit a přejít na plochu, ale očekávaný průběh této operace je narušen reklamou.

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).

Příklad běžného porušení zásad:



- ① Tato reklama (pro mládež) není vhodná pro cílové publikum této aplikace (7+)
- ② Tato reklama (pro dospělé) není vhodná pro cílové publikum této aplikace (12+)

Použití inzertního 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:** Inzertní 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 k jiným identifikátorům**
 - Použití pro inzerci: Inzertní identifikátor nesmí být přidružen k trvalým identifikátorům zařízení (například k SSAID, MAC adrese, IMEI apod.) k žádnému reklamnímu účelu. Inzertní identifikátor smí být k údajům umožňujícím zjištění totožnosti přidružen pouze s výslovným souhlasem uživatele.
 - Použití pro analýzy: Inzertní identifikátor smí být přidružen k informacím, které umožňují zjištění totožnosti, nebo k trvalému identifikátoru zařízení (například SSAID, MAC adresa, číslo IMEI apod.) pouze s výslovným souhlasem uživatele.
- **Respektování voleb uživatelů.** Po resetování nesmí být nový inzertní identifikátor bez výslovného souhlasu uživatele přidružen k předchozímu inzertnímu 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 inzertní 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 inzertního 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.** Inzertní identifikátor je dovoleno používat pouze v souladu s těmito smluvními podmínkami. Tyto smluvní podmínky musejí dodržovat všechny strany, se kterými inzertní 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).

Reklamy v programu Pro celou rodinu

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 ohledně údajů o uživateli](#) a [zásadami pro rodiny](#) služby Play:

- Vlastní inzerce, při které používáte sady SDK k propagaci svých vlastních aplikací, médií či reklamního zboží
- Přímé dohody s inzerenty, při kterých využíváte sady 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 měly splňovat programové zásady služby Play pro vývojáře.
- Vytvořte metodu k hodnocení kreativy podle věkových skupin. Věkové skupiny musí obsahovat 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. Obsah určený dětem musí být v souladu s příslušnými zákony a jinými právními předpisy, 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 reklamních sad SDK určených pro děti byly deaktivovány personalizované reklamy, zájmově orientované reklamy a remarketing.
- Majitelé stránek mohou vybrat formáty reklam, které jsou v souladu se [zásadami služby Play ohledně reklam a zpeněžení pro rodiny](#) a splňují požadavky [programu Schváleno učiteli](#).
- 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 (např. informace ve [formuláři pro zájemce](#) uvedeném níže), aby mohla ověřit, 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 informace potřebné k tomu, aby mediační platformy určily hodnocení obsahu reklamy a případného obsahu určeného dětem.

Zde si mohou vývojáři projít [seznam certifikovaných sad SDK](#).

Poskytovatele reklamních sad SDK, kteří chtějí získat vlastní certifikaci, mohou vývojáři také odkázat na tento [formulář pro zájemce](#).

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 aplikace. V popisu aplikace je také zakázáno uvádět anonymní nebo nepřirazená prohlášení uživatelů.

Kromě zde uvedených požadavků mohou určité zásady pro vývojáře ve službě Play vyžadovat poskytnutí dalších metadat.

Příklady běžných porušení zásad:

RescueRover

The best way to find a new furry friend!

RescueRover lets you use your Android device to search for rescue dogs.

1

See how much our users love us:

"It was easy to find the right dog for me and my family!"

2

It's the #1 app after Pet Rescue Saga, but in real life!

50% cooler and 100% faster than FidoFinder

3

You can see black dogs, brown dogs, white dogs, big dogs, medium dogs, small dogs, dog leashes, dog training books, dog bowls, dog toys, dog accessories. dog, dogs, rescue, shelter, animal, pet, pets, adopt, foster, puppy, puppies, dogs including:

- 1) golden retriever
- 2) labradoodle
- 3) poodle
- 4) chihuahua
- 5) akita
- 6) pug
- 7) rottweiler



- 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 sexuální podtextem. Nepoužívejte reálné ani ilustrované obrázky se sexuální podtextem, které vyobrazují ňadra, hýždě, genitálie ani jiné části těla či obsah, který může být předmětem sexuálního vzrušení.
- Vulgární, neslušné a jiné výrazy, které nejsou vhodné pro obecné publikum.
- 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.

Několik doporučených postupů:

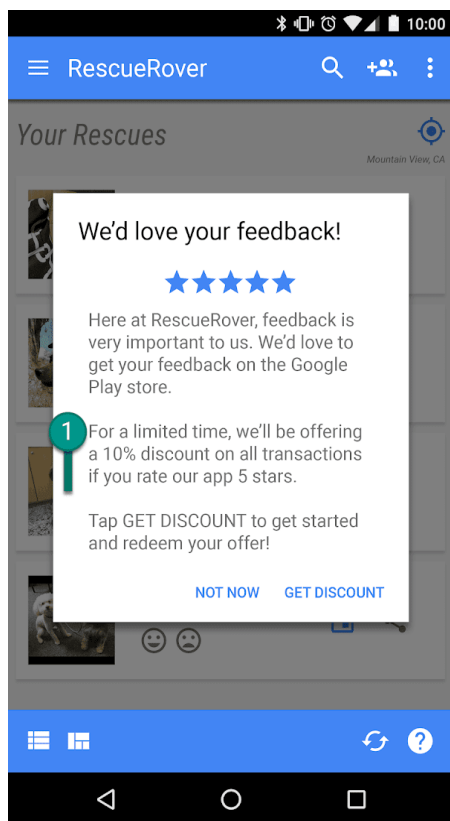
- Zdůrazněte, co je na vaší aplikaci skvělého. Podělte se s uživateli o zajímavá a poutavá fakta, aby vaši aplikaci snáze odlišili od konkurence.
- Název a popis aplikace musí přesně popisovat její funkce.
- Nepoužívejte opakující se ani nesouvisející klíčová slova a reference.
- Popis aplikace by měl 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.

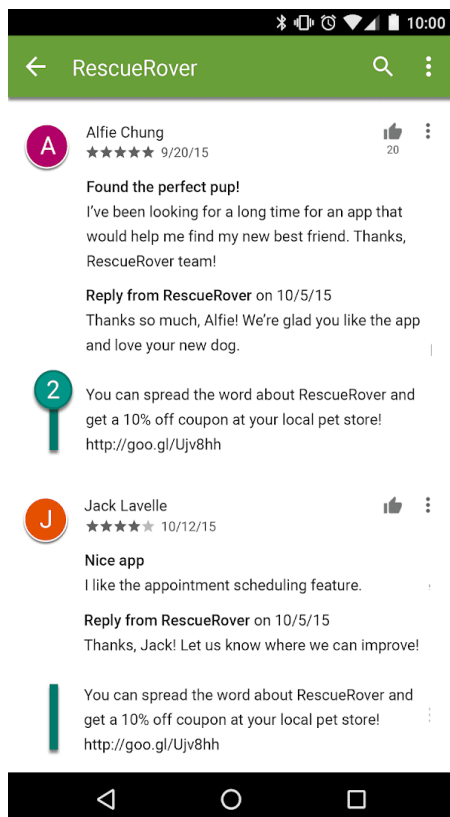
Příklady běžných porušení zásad:

- 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

Hodnocení obsahu na Google Play obsahuje oficiální hodnocení od organizace IARC (International Age Rating Coalition) a jeho cílem je pomoci vývojářům informovat uživatele o hodnocení místně relevantního obsahu. Místní autority IARC se řídí pravidly určenými ke stanovení úrovně vhodnosti obsahu v aplikaci pro určitou věkovou skupinu. Aplikace bez hodnocení obsahu nejsou v Google Play povoleny.

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 hodnotících 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.

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

Další informace o různých [hodnotících 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 hodnotícího orgánu IARC pomocí odkazu v e-mailu s certifikátem hodnocení.

Zprávy

Aplikace, které jsou na Google Play deklarovány jako zpravodajské, musí splňovat všechny následující požadavky.

Zpravodajské aplikace vyžadující zakoupení členství musí uživateli před zakoupením poskytnout náhled obsahu.

Zpravodajské aplikace MUSÍ:

- poskytnout informace o vlastnictví v souvislosti s vydavatelem zpráv a jeho přispěvateli, mimo jiné včetně oficiálního webu pro zprávy publikované v aplikaci, platných a ověřitelných kontaktních údajů a původního vydavatele jednotlivých článků,
- mít webovou stránku nebo stránku v aplikaci, která poskytuje platné kontaktní údaje na vydavatele zpráv.

Zpravodajské aplikace NESMÍ:

- obsahovat výrazné gramatické a pravopisné chyby,
- obsahovat výhradně statický obsah (např. obsah starý několik měsíců),
- mít jako hlavní účel affiliate marketing nebo tržby z reklam.

Zpravodajské aplikace, které agregují obsah z různých zdrojů, musí jasně informovat o zdroji obsahu publikovaného v aplikaci a každý ze zdrojů musí splňovat požadavky zásad pro Zprávy.

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

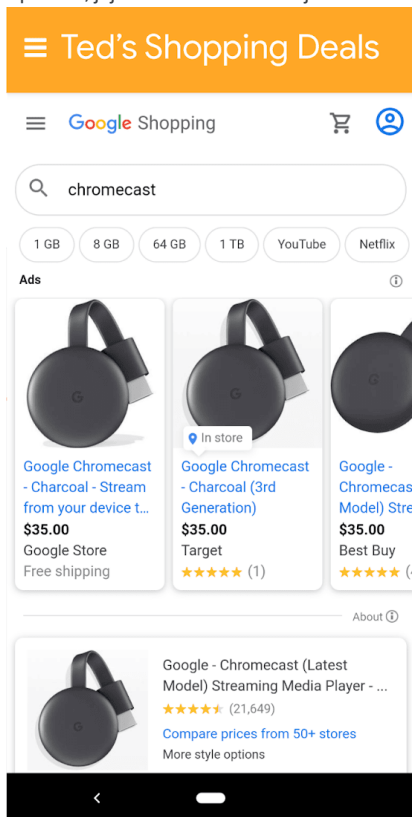
Nepovolujeme aplikace, které rozesílají SMS zprávy, e-maily nebo jiné zprávy jménem jiného uživatele, aniž by tento uživatel mohl potvrdit obsah a příjemce zprávy.

Spam zvyšující návštěvnost

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

Příklady běžných porušení zásad:

- 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 bez svolení poskytovat zobrazení webu:



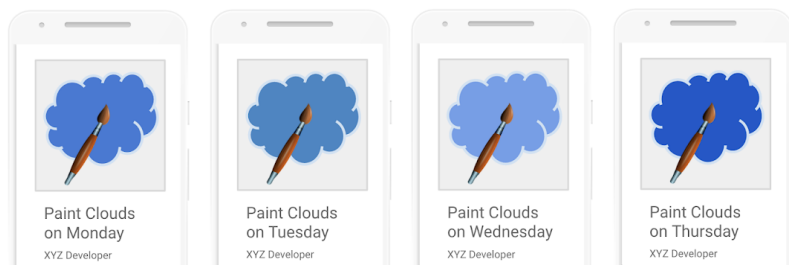
Tato aplikace se nazývá „Tedovy nákupní nabídky“ a nabízí pouze zobrazení webu Nákupů Google.

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.

Příklady běžných porušení zásad:

- kopírování obsahu z jiných aplikací bez přidání originální 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.



Vytvořeno pro reklamy

Nepovolujeme aplikace, jejichž primárním účelem je zobrazování reklam.

Příklady běžných porušení zásad:

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

Minimální funkčnost

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

Příklady běžných porušení zásad:

- Aplikace, které nemají žádný účel ani funkci.

Poruchy funkčnosti

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

Příklady běžných porušení zásad:

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

Další programy

Kromě dodržování obsahových zásad stanovených jinde v tomto centru zásad se na aplikace určené pro ostatní prostředí Android a distribuované prostřednictvím Google Play mohou vztahovat také zásady konkrétního programu. Chcete-li zjistit, zda se některé z těchto zásad na vaši aplikaci vztahují, prohlédněte si níže uvedený seznam.

Okamžité aplikace Android

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

Identita

U okamžitých aplikací, které obsahují funkci přihlášení, musí vývojáři integrovat funkci [Smart Lock na hesla](#).

Podpora odkazů

Vývojáři okamžitých aplikací Android musí poskytovat náležitou podporu pro odkazy na ostatní aplikace. Pokud vývojářova okamžitá aplikace nebo instalovaná aplikace obsahuje 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 průběžně upravovány, 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 informace o okamžitých aplikacích a pokyny k uživatelskému rozhraní naleznete v [doporučených postupech k uživatelskému prostředí](#).

Změna stavu zařízení

Okamžitá 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 okamžitá aplikace byly pro uživatele viditelné a uživatel si byl po celou dobu vědom, že je v jeho zařízení spuštěna okamžitá aplikace.

Identifikátory zařízení

Okamžitá 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.

Okamžitá 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 vaše aplikace cílí na děti i na starší publikum, do programu Pro celou rodinu se můžete stále zapojit. Všechny aplikace, které se přihlásí do programu Pro celou rodinu, budou způsobilé pro hodnocení v rámci programu [Schváleno učiteli](#). Nemůžeme však zaručit, že aplikace bude do programu Schváleno učiteli zařazena. 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 vybrané věkové skupiny 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 můžete kdykoliv aktualizovat v sekci Cílové publikum a obsah v Google Play. 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 uvádět 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.

- Obsah aplikace:** Obsah aplikace přístupný dětem musí být pro děti vhodný.
- Odpovědi v Google Play Console:** Na otázky ohledně aplikace v Google Play Console musíte pravdivě odpovídat a aktualizovat je tak, aby přesně reflektovaly veškeré změny aplikace.
- 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 (reklamy cílené na uživatele s určitými vlastnostmi na základě chování při procházení webů) ani se nejednalo o remarketing (reklamy cílené na jednotlivé uživatele na základě předchozí interakce s aplikací nebo webem),
 - 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.
- 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, data z mikrofonu a ze senzorů kamery, údaje o zařízení, Android ID, údaje o využití reklam a inzertní ID.
- 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 na 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 údajů od dětí (např. přihlášení přes Google poskytovat jako volitelnou funkci). Aplikace, které cílí na děti i na starší publikum, nesmí vyžadovat přihlášení k obsahu ani k přístupu k obsahu aplikace prostřednictvím rozhraní API nebo sady SDK, které nejsou schváleny ve službách určených pro děti.

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.

Příklady běžných porušení zásad:

- 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 regulovaných 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 obsahují odkazy na webové stránky s obsahem, který porušuje [Programové zásady pro vývojáře](#) Google Play.
- aplikace, které dětem zobrazují reklamy určené pouze dospělým (např. násilný obsah, sexuální obsah, obsah týkající se hazardních her). Další informace naleznete v [zásadách reklam a zpeněžení Pro celou rodinu](#), kde naleznete informace o zásadách služby Google Play ohledně inzerce, nákupů v aplikacích a komerčního obsahu pro děti.

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](#) splňovat i všechny požadavky zásad pro rodiny a podmínky způsobilosti k účasti v programu Pro celou rodinu.

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

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 může odmítnout, odstranit nebo pozastavit 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 smí 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 musí používat [Správce doprovodných zařízení \(CDM\)](#) (kromě aplikací, jež cílí pouze na verze operačního systému zařízení, které se Správcem 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.
- aplikace, které používají ikonu aplikace nebo ikonu spouštěče, která není vhodná pro děti.

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 dobrodružství: 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 podněcují 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 ve vaší aplikaci (včetně reklam na vaše aplikace a aplikace třetích stran), nabídky nákupů v aplikaci a na veškerý další komerční obsah (například placené zobrazení produktu) 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 zákony a jinými právními předpisy (včetně relevantních zásad samoregulace a standardů v odvětví).

Google Play si vyhrazuje právo odmítnout, odstranit nebo pozastavit aplikace, které používají příliš agresivní obchodní taktiky.

Podmínky pro formát reklam

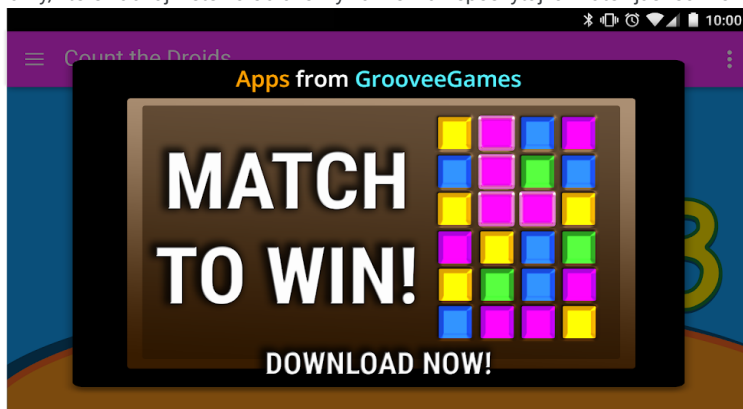
Reklamy a nabídky nákupů v aplikacích nesmí mít klamavý obsah a nesmí být navrženy způsobem, který by měl za následek neúmyslná kliknutí dětských uživatelů. Jsou zakázány následující praktiky:

- rušivé reklamy, například takové, které zaberou celou obrazovku nebo jinak brání běžné práci s aplikací a neposkytují jasně viditelnou možnost reklamu zavřít (např. [přístup podmíněný reklamou](#)),
- reklamy, které narušují běžné používání aplikace nebo hry a které nelze zavřít po uplynutí 5 sekund, reklamy, které nenarušují běžné používání aplikace nebo hry se mohou zobrazovat i déle než 5 sekund (např. videoobsah s integrovanými reklamami),
- zobrazování vsunutých reklam nebo nabídek nákupů v aplikaci ihned po spuštění aplikace,
- umístění více reklam na stránce (nepovolujeme například bannerové reklamy, které zobrazují více nabídek v jednom umístění, nebo zobrazování více než jednoho banneru či videoreklamy),
- 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 nákupům v aplikaci,
- nerozlišování virtuální herní měny a reálných peněz u nákupů v aplikacích.

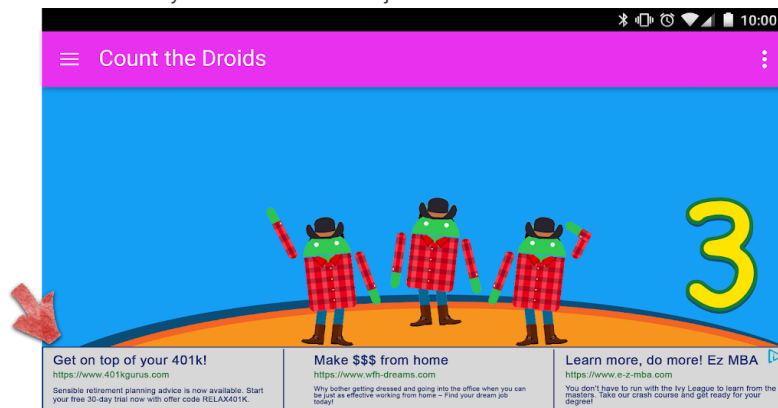
Příklady běžných porušení zásad ohledně formátu reklamy:

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

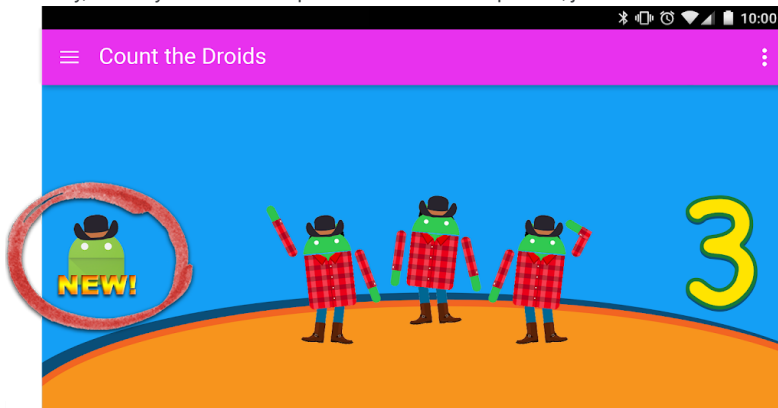
- Reklamy, které zabírají většinu obrazovky zařízení a neposkytují uživateli jasnou možnost zavření, jako na obrázku níže:



- Bannerové reklamy s několika nabídkami jako na obrázku níže:

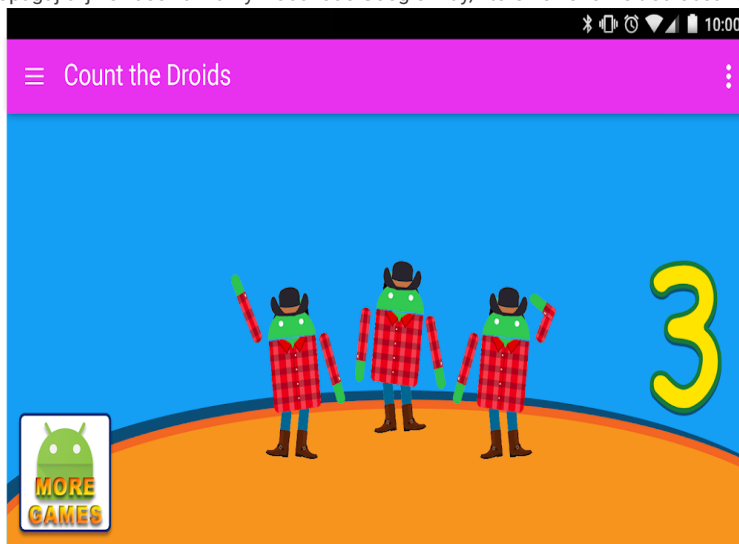


- Reklamy, které by uživatel mohl považovat za obsah aplikace, jako na obrázku níže:



- 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

Pokud v aplikaci zobrazujete reklamy a cílíte pouze na děti, musíte používat [sady SDK pro reklamy certifikované službou Google Play](#). Pokud vaše aplikace cílí na děti i na starší uživatele, musíte implementovat opatření na filtrování podle věku uživatelů, například [neutrální věkový filtr](#), a zajistit, aby reklamy zobrazované dětem pocházely výhradně z reklamních sad SDK certifikovaných službou Google Play. Aplikace v programu Pro celou rodinu mohou používat pouze reklamní sady SDK s vlastní certifikací.

Další informace 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 jejich 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 svého poskytovatele reklamních sad SDK, obraťte se přímo na něj.

Nákupy v aplikaci

V aplikacích zařazených do programu Pro celou rodinu bude služba Google Play před všemi nákupy v aplikaci každého uživatele znovu ověřovat. Cílem tohoto opatření je zajistit, aby nákupy schvalovaly 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 uživateli 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](#).

Nepovolujeme aplikace ani obsah aplikací podřývajících důvěru uživatelů v ekosystém Google Play. Při rozhodování, zda zahrnout nebo odstranit aplikaci z Google Play, zvažujeme různé faktory, mezi které patří mimo jiné podezření na škodlivé chování nebo vysoké riziko zneužití. Riziko zneužití identifikujeme mimo jiné na základě stížností na konkrétní aplikace nebo vývojáře, zpravodajství, porušení zásad v minulosti, zpětné vazby uživatelů nebo použití populárních značek, postav nebo jiných položek.

Jak Google Play Protect funguje

Google Play Protect kontroluje aplikace, které instalujete. Pravidelně také prochází vaše zařízení. Pokud nalezne potenciálně škodlivou aplikaci, může provést následující akce:

- Pošle vám oznámení. Budete-li chtít aplikaci odstranit, klepněte na oznámení a poté na Odinstalovat.
- Aplikaci deaktivuje, dokud ji neodinstalujete.
- Odstraní aplikaci automaticky. Ve většině případů se vám po zjištění škodlivé aplikace zobrazí oznámení, že aplikace byla odstraněna.

Jak funguje ochrana před malwarem

Za účelem ochrany před škodlivým softwarem či adresami URL třetích stran a jinými bezpečnostními problémy může společnost Google dostávat informace o:

- připojení vašeho zařízení k sítím,
- potenciálně škodlivých adresách URL,
- operačním systémem a aplikacích nainstalovaných na vaše zařízení z Google Play nebo jiných zdrojů.

Google vám může zobrazit oznámení, že nějaká aplikace nebo adresa URL je potenciálně nebezpečná. Pokud je známo, že aplikace nebo adresa URL poškozuje zařízení, data nebo uživatele, Google ji může odstranit nebo zablokovat.

Některé z těchto ochranných opatření můžete v nastavení svého zařízení vypnout. Společnost Google však může i nadále dostávat informace o aplikacích nainstalovaných prostřednictvím Google Play a aplikace nainstalované na zařízení z jiných zdrojů mohou být kontrolovány za účelem zjištění případných bezpečnostních problémů bez odesílání informací do Googlu.

Jak fungují upozornění na ochranu soukromí

Google Play Protect vás upozorní, pokud je aplikace odstraněna z Obchodu Google Play, protože měla přístup k vašim osobním údajům. Takovou aplikaci budete mít možnost odinstalovat.

Proces uplatňování zásad

Pokud vaše aplikace porušuje některou z našich zásad, podnikneme odpovídající opatření, jak je uvedeno níže. Poskytneme vám také relevantní informace o podniknutých opatřeních, které vám zašleme e-mailem, a pokyny, jak se odvolat, pokud jste přesvědčeni, že jsme tato opatření proti vám podnikli omylem.

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 problémů týkajících se porušení zásad. Zároveň se očekává, že věnujete zvýšenou pozornost tomu, aby zásadám plně odpovídala i zbývající část aplikace. Pokud nevyřešíte porušení zásad ve všech svých aplikacích, můžeme proti vám podniknout další kroky.

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).

Donucovací opatření

Proti vaší aplikaci mohou být podniknuta různá donucovací opatření. Následující sekce popisuje různá opatření, která může služba Google Play podniknout, a jak tato opatření mohou ovlivnit vaši aplikaci nebo účet vývojáře Google Play. Tyto informace jsou vysvětleny také v [tomto videu](#).

Zamítnutí

- Nová aplikace nebo aktualizace aplikace odeslaná ke kontrole nebude na Google Play k dispozici.
- Pokud byla zamítnuta aktualizace stávající, verze aplikace publikovaná před touto aktualizací zůstane na Google Play dostupná i nadále.
- Zamítnutí nemá vliv na přístup k existujícím uživatelským instalacím, statistikám a hodnocení zamítnuté aplikace.
- Zamítnutí nemá vliv na pověst vašeho účtu vývojáře Google Play.

Poznámka: Nesnažte se zamítnutou aplikaci znovu odeslat, dokud neodstraníte všechna porušení zásad.

Odstranění

- Aplikace bude i s případnými předchozími verzemi odstraněna z Google Play a uživatelé ji už nebudou moci stáhnout.
- Protože byla aplikace odstraněna, uživatelé neuvidí její záznam v obchodu, počet instalací (uživatelů), statistiky ani hodnocení. Tyto informace se obnoví, jakmile pro danou aplikaci odešlete aktualizaci, která bude v souladu se zásadami.
- Uživatelé možná nebudou moci provádět nákupy v aplikaci ani používat funkce fakturace v aplikaci, dokud služba Google Play neschválí verzi, která bude v souladu se zásadami.
- Odstranění nemusí okamžitě ovlivnit pověst vašeho účtu vývojáře Google Play, vícenásobné odstranění však může vést k tomu, že bude váš účet pozastaven.

Poznámka: Nesnažte se odstraněnou aplikaci znovu zveřejňovat, dokud nenapравíte všechna porušení zásad.

Pozastavení

- Aplikace bude i se všemi svými předchozími verzemi odstraněna z Google Play a uživatelé ji už nebudou moci stáhnout.
- K pozastavení může dojít v důsledku vážného nebo vícenásobného porušení zásad nebo opakovaného zamítnutí či odstranění aplikací.
- Protože aplikace byla pozastavena, uživatelé neuvidí její záznam v obchodu, stávající počet instalací (uživatelů), statistiky ani hodnocení. Tyto informace se obnoví, jakmile odešlete aktualizaci, která bude v souladu se zásadami.
- Soubor APK ani balíček pozastavené aplikace už nelze používat.
- Uživatelé nebudou moci provádět nákupy v aplikaci ani používat funkce fakturace v aplikaci, dokud služba Google Play neschválí verzi, která bude v souladu se zásadami.
- Pozastavení poškozují dobrou pověst vašeho účtu vývojáře Google Play. Větší počet sankcí může vést k ukončení jednotlivých i souvisejících účtů vývojáře Google Play.

Poznámka: Nepokoušejte se pozastavenou aplikaci znovu publikovat, dokud vám to Google Play nepovolí.

Omezená viditelnost

- Objektivnost aplikace na Google Play je omezena. Aplikace bude na Google Play nadále dostupná a uživatelé k ní budou mít přístup pomocí přímého odkazu na záznam aplikace v Obchodu Play.
- Omezení viditelnosti aplikace nijak neovlivní pověst vašeho účtu vývojáře Google Play.
- U aplikace, jejíž viditelnost byla omezena, mohou uživatelé i nadále zobrazit její existující záznam v obchodu, počet instalací (uživatelů), statistiky či hodnocení.

Ukončení účtu

- Až bude váš účet vývojáře ukončen, všechny aplikace z vašeho katalogu budou z Google Play odstraněny a vy již nebudete moci publikovat nové. To znamená, že budou trvale pozastaveny i všechny související účty vývojáře Google Play.
- Vícenásobné pozastavení nebo pozastavení z důvodu hrubého porušení zásad také může vést k ukončení účtu Play Console.
- Protože aplikace z ukončeného účtu budou odstraněny, uživatelé neuvidí jejich záznamy v obchodu, stávající počet instalací (uživatelů), statistiky ani hodnocení.

Poznámka: Pokud se pokusíte otevřít nové účty, budou také ukončeny (bez vrácení poplatku za registraci vývojáře). Proto se nepokoušejte zaregistrovat nový účet Play Console, pokud je některý z vašich jiných účtů ukončen.

Správa a hlášení porušení zásad

How to handle a policy violation on Go...



Odvolání proti donucovacím opatřením

Pokud dojde k chybě a zjistíme, že vaše aplikace neporušuje programové zásady služby Google Play ani distribuční smlouvu pro vývojáře, aplikaci obnovíme. Pokud jste si zásady pečlivě přečetli a domníváte se, že naše rozhodnutí mohlo být chybné, postupujte podle pokynů, které najdete v e-mailu s oznámením o donucovacím opatření a s jejichž pomocí se můžete proti našemu rozhodnutí odvolat.

Další zdroje

Pokud potřebujete další informace ohledně donucovacích opatření nebo hodnocení či komentářů od uživatele, můžete si prohlédnout některý z níže uvedených zdrojů nebo nás kontaktovat prostřednictvím [centra nápovědy služby Google Play](#). Neposkytujeme však právní poradenství. Pokud ho potřebujete, obraťte se na svého 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](#)

Potřebujete další pomoc?

Vyzkoušejte tyto další kroky:

Kontaktujte nás

Řekněte nám víc a my vám pomůžeme