Programové zásady pro vývojáře

(platné od 31. srpna 2024, pokud není uvedeno jinak)

Usilujme společně o nejdůvěryhodnější zdroj aplikací a her

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

Zakázaný obsah

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

Ohrožení dětí

Aplikace, které uživatelům nezakazují vytvářet, nahrávat nebo distribuovat obsah, který umožňuje využívání nebo obtěžování dětí, budou z Google Play okamžitě odstraněny. To zahrnuje všechny materiály zobrazující sexuální zneužívání dětí. Pokud v některé službě Google chcete nahlásit obsah, který může zneužívat děti, klikněte na **Nahlásit zneužití** . Pokud takový obsah najdete kdekoli jinde na internetu, obraťte se přímo na příslušný úřad ve vaší zemi .

Zakazujeme používání aplikací k ohrožování dětí. Patří sem mimo jiné používání aplikací k propagaci agresivního chování vůči dětem, jako jsou:

- nevhodná interakce s nezletilými (např. osahávání),
- tzv. lákání dětí (například navázání přátelství s dítětem na internetu s cílem otevřít si cestu k sexuálním kontaktům na internetu i mimo něj nebo k výměně sexuálně laděných obrazových materiálů),
- sexualizace dětí (např. obrázky, které znázorňují, podporují nebo propagují sexuální zneužívání dětí, případně děti vyobrazují v situacích, které mohou vést k sexuálnímu zneužívání),
- vydírání související se sexem (například vyhrožování dítěti nebo jeho vydírání na základě skutečného nebo údajného přístupu k intimním obrázkům dítěte),
- obchodování s dětmi (například reklama nebo nabízení dítěte ke komerčnímu sexuálnímu vykořisťování).

Pokud se dozvíme o materiálech zobrazujících sexuální zneužívání dětí, podnikneme příslušné kroky, které mohou zahrnovat nahlášení organizaci National Center for Missing & Exploited Children. Pokud se domníváte, že je nějaké dítě v nebezpečí nebo že bylo vystaveno obtěžování, zneužívání nebo obchodování s lidmi, obraťte se na místní bezpečnostní složky a na organizaci pro ochranu dětí uvedenou zde .

Kromě toho nejsou povoleny aplikace, které jsou přitažlivé pro děti, ale obsahují témata pro dospělé, mimo jiné:

- aplikace s nadměrnou mírou násilí a krvavých scén,
- aplikace, které zobrazují nebo podporují škodlivé a nebezpečné aktivity.

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.

Nevhodný obsah

Aby platforma Google Play zůstala bezpečná a zdvořilá, 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. Nepovolujeme aplikace ani obsah aplikací, který lze vykládat jako propagaci nebo nabízení sexuálního jednání za úplatu. Nepovolujeme aplikace, které zahrnují nebo propagují obsah spojený se sexuálně agresivním chováním nebo distribuují nedobrovolný sexuální obsah. Obsah zahrnující nahotu může být povolen v případě, že má primárně vzdělávací, dokumentární, vědecký či umělecký účel a nahota v něm není bezdůvodná.

Katalogové aplikace – aplikace, které obsahují seznam knih/videí v rámci širšího katalogu obsahu – mohou distribuovat knihy (včetně e-knih a audioknih) nebo videa se sexuálním obsahem, pokud jsou splněny následující požadavky:

- Knihy/videa se sexuálním obsahem představují jen malou část celkového katalogu aplikace.
- Aplikace knihy/videa se sexuálním obsahem aktivně nepropaguje. Takovéto knihy/videa se však mohou zobrazovat v doporučeních na základě historie uživatele nebo během obecných cenových promoakcí.
- Aplikace nedistribuuje žádnou knihu/video s obsahem ohrožujícím děti, pornografickým obsahem ani jiným sexuálním obsahem, který podle platných právních předpisů není legální.
- Aplikace chrání nezletilé tím, že ke knihám/videím se sexuálním obsahem omezuje přístup.

Pokud obsah aplikace porušuje tyto zásady, ale v dané oblasti je považován za vhodný, aplikace může být k dispozici pro uživatele v dané oblasti, ale zůstane nedostupná pro uživatele z jiných oblastí.

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.
- Obscénní či sprostý obsah (např. obsah, který může v záznamu v obchodu nebo v samotné 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 nebo vyžadování sexuálních služeb za peníze, mimo jiné včetně placených schůzek nebo dohod sexuální povahy, kdy se od jednoho účastníka očekávají peníze, dárky nebo finanční podpora pro druhého účastníka („sugar dating“).
- Aplikace, které lidi ponižují nebo objektifikují, např. aplikace, které tvrdí, že umožňují vidět lidi svlečené nebo se dívat lidem skrz oblečení (a to i v případě, že jsou tyto aplikace označené jako žertovné nebo zábavné).
- Obsah nebo chování, které se pokouší ohrožovat nebo zneužívat lidi sexuálním způsobem, jako jsou tajně pořízené záběry se sexuálním podtextem, skryté kamery, nedobrovolný sexuální obsah vytvořený pomocí technologie deepfake či jiné podobné technologie nebo obsah zachycující sexuální napadení.

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, kasty, statusu imigranta ani jakékoli 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 nenávist.
- 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 nenávist.

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:

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

Násilný extremismus

Teroristickým organizacím ani jiným nebezpečným organizacím či hnutím, které se zapojily do násilných činů proti civilistům, připravovaly se na ně nebo se k nim přihlásily, nepovolujeme publikovat aplikace na Google Play za žádným účelem, zejména ne k náboru členů.

Nepovolujeme aplikace s obsahem, který souvisí s násilným extremismem nebo plánováním, přípravou či oslavováním násilí proti civilistům (tj. například podněcuje k teroristickým činům či násilí nebo oslavuje teroristické útoky). Pokud sdílíte obsah související s násilným extremismem ve vzdělávacím, dokumentárním, vědeckém nebo uměleckém kontextu, vždy k němu poskytněte dostatek souvislostí.

Citlivé události

Nepovolujeme aplikace, které vydělávají na citlivých událostech s významným sociálním, kulturním nebo politickým dopadem, jako jsou společenské nepokoje, přírodní katastrofy, mimořádné události v oblasti veřejného zdraví, konflikty, úmrtí nebo jiné tragické události, nebo k takovým událostem nejsou citlivé. 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 dobře zdokumentované závažné tragické události.

- Zjevný pokus o profitování na citlivé události bez zřejmého užitku pro oběti.

Šikana a obtěžování

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

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 tabáku nebo produktů obsahujících nikotin (jako jsou elektronické cigarety, vaporizační pera a nikotinové sáčky) nebo podporují nezákonné či nevhodné užívání alkoholu, tabáku nebo nikotinu.

Další informace

- Vyobrazení nebo propagace užívání či prodeje alkoholu nebo tabáku nezletilými nejsou povoleny.
- Naznačování, že konzumace tabákových výrobků může zlepšit společenský, sexuální, profesionální, duševní či tělesný stav, není povoleno.
- Pozitivní prezentace nadměrného pití, včetně zobrazování nadměrného a nestřídmého pití či závodů v pití v pozitivním světle, není povolena.
- Inzerce, propagace nebo vyzdvihování tabákových výrobků (včetně reklam, bannerů, kategorií a odkazů na weby prodávající tabák) nejsou povoleny.
- Může být dovolen omezený prodej tabákových výrobků v aplikacích na doručování potravin, a to jen v určitých oblastech a s nutností ověření věku a dalších bezpečnostních opatření (např. předložení občanského průkazu při dodání).

- Může být povolen prodej produktů, které jsou nabízeny jako pomůcky k odvykání nikotinu, pokud jsou přijata náležitá bezpečnostní opatření s ověřením věku.

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.)

Pro každou aplikaci, která obsahuje finanční funkce, je třeba v Play Console vyplnit deklarační formulář finančních funkcí.

Binární opce

Nepovolujeme aplikace, které uživatelům umožňují obchodovat s binárními opcemi.

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 finančních produktů, 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, 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 mít v Play Console nastavenou kategorii Finance a musí v metadatech aplikace uvést následující informace:

- minimální a maximální dobu splácení,
- maximální roční procentní 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 jistiny a všech souvisejících poplatků,
- zásady ochrany osobních údajů, které komplexně popisují přístup k osobním a citlivým uživatelským údajům a jejich shromažďování, používání a sdílení v souladu s omezeními uvedenými v těchto zásadách.

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“).

Výjimky z této zásady budou zváženy u aplikací pro osobní půjčky provozované v zemích, kde konkrétní předpisy výslovně povolují poskytování takovýchto krátkodobých půjček v souladu se zavedenými právními rámci. V těchto vzácných případech budou výjimky posouzeny v souladu s platnými místními právními předpisy a regulačními směrnicemi příslušné země.

Musíme být schopni identifikovat spojení mezi vaším účtem vývojáře a veškerými poskytnutými licencemi nebo dokumentací prokazující vaši schopnost poskytovat osobní půjčky. K potvrzení, že je

váš účet v souladu se všemi místními zákony a předpisy, mohou být vyžadovány další informace nebo dokumenty.

Aplikace pro osobní půjčky, aplikace, jejichž primárním účelem je usnadnit přístup k osobním půjčkám (například oslovují potenciální zákazníky nebo působí jako zprostředkovatelé), pomocné aplikace související s půjčkami (například úvěrové kalkulačky či průvodci) a aplikace typu „výplata kdykoliv“ (Earned Wage Access) mají zakázán přístup k citlivým údajům, jako jsou fotografie a kontakty. Jsou zakázána následující oprávnění:

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

Na aplikace, které používají citlivé údaje nebo citlivá rozhraní API, se vztahují další omezení a požadavky. Další informace najdete v zásadách pro oprávnění.

Osobní půjčky s vysokou RPSN

V USA nepovolujeme aplikace pro osobní půjčky, u nichž roční procentní 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.

Požadavky platné pro jednotlivé země

Aplikace na osobní půjčky, které cílí na uvedené země, musí splňovat další požadavky a v rámci deklarace finančních funkcí v Play Console poskytnout dodatečnou dokumentaci. Na žádost služby Google Play musíte poskytnout další informace nebo dokumenty související s vaším dodržováním příslušných zákonných a licenčních požadavků.

1. **Indie**
   - Pokud vám Reserve Bank of India udělila licenci k poskytování osobních půjček, odešlete nám kopii této licence ke kontrole.
   - Pokud přímo neposkytujete peněžní půjčky, ale pouze nabízíte platformu k usnadnění půjčování peněz bankami nebo registrovanými nebankovními peněžními společnostmi uživatelům, je třeba to v deklaraci patřičně uvést.
     - Je také nutné v aplikaci viditelně uvést názvy všech registrovaných bank a nebankovních peněžních společností.
2. **Indonésie**
   - Pokud vaše aplikace zprostředkovává služby peněžních půjček na základě informačních technologií v souladu s nařízením OJK č. 77/POJK.01/2016 (které může být průběžně novelizováno), je třeba, abyste nám odeslali ke kontrole kopii své platné licence.
3. **Filipíny**
   - Všechny finanční a půjčkové společnosti, které nabízejí úvěry prostřednictvím online půjčkových platforem, musejí od filipínské komise pro obligace a burzy získat registrační číslo SEC a certifikát oprávnění.
     - V popisu aplikace musejí také uvést název společnosti, registrační číslo PSEC a certifikát oprávnění provozovat finanční nebo půjčkovou společnost.

- Aplikace, které poskytují půjčky na základě crowdfundingu (např. půjčky mezi jednotlivci) nebo které spadají pod definici v Pravidlech a nařízeních o crowdfundingu (CF Rules), musejí zpracovávat transakce skrze zprostředkovatele zaregistrované u úřadu PSEC.

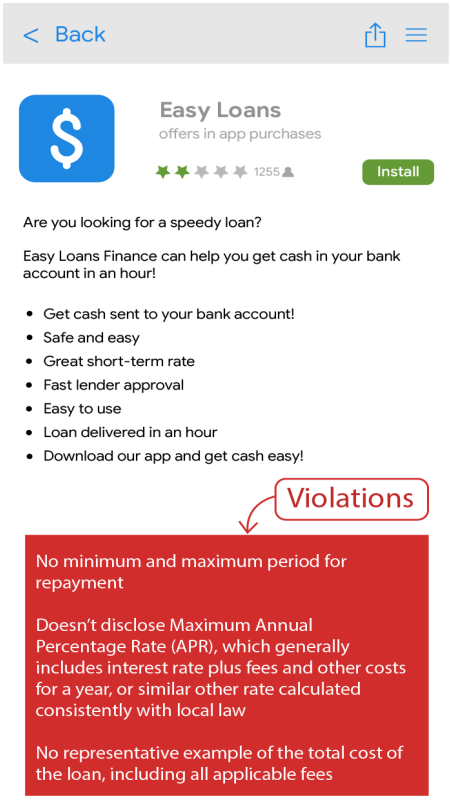
4. **Nigérie**
   - Poskytovatelé digitálních půjček musí splňovat OMEZENÝ DOČASNÝ REGULAČNĚ-REGISTRAČNÍ RÁMEC A SMĚRNICE PRO DIGITÁLNÍ PŮJČKY z roku 2022 (které mohou být průběžně pozměňovány) vydané nigerijskou Federální komisí pro hospodářskou soutěž a ochranu spotřebitelů (FCCPC) a získat od FCCPC ověřitelný schvalovací dopis.
   - Agregátory půjček musí poskytnout dokumentaci a/nebo certifikaci o poskytování digitálních půjček a kontaktní údaje jednotlivých poskytovatelů.

5. **Keňa**
   - Poskytovatelé digitálních úvěrů musí dokončit registraci a získat licenci od Keňské centrální banky (CBK). V rámci deklarace musíte předložit kopii licence od banky CBK.
   - Pokud přímo neposkytujete peněžní půjčky, ale pouze nabízíte platformu k usnadnění půjčování peněz poskytovateli digitálních úvěrů uživatelům, je třeba to v deklaraci patřičně uvést a poskytnout kopii licencí poskytovatele digitálních úvěrů patřících příslušným partnerům.
   - Momentálně přijímáme pouze deklarace a licence od subjektů zveřejněných v rejstříku poskytovatelů digitálních úvěrů na oficiálním webu CBK.

6. **Pákistán**
   - Každá nebankovní finanční společnost (Non-Banking Finance Company – NBFC), která poskytuje půjčky, může publikovat pouze jednu aplikaci pro digitální poskytování půjček (Digital Lending App – DLA). Vývojáři, kteří se pokusí publikovat více než jednu aplikaci DLA na jednu společnost NBFC, se vystavují riziku ukončení účtu vývojáře a všech dalších přidružených účtů.
   - Pokud v Pákistánu chcete nabízet nebo zprostředkovávat digitální služby poskytování půjček, musíte poskytnout doklad o schválení od úřadu SECP.

7. **Thajsko**
   - Aplikace pro osobní půjčky s úrokovými sazbami 15 % nebo vyššími, které cílí na Thajsko, musí získat platnou licenci od Thajské centrální banky (BoT) nebo od Ministerstva financí (MoF). Vývojáři musí poskytnout dokumentaci, která potvrzuje, že smí poskytovat nebo zprostředkovávat osobní půjčky v Thajsku. Tato dokumentace musí zahrnovat:
     - Kopii licence vydané Thajskou centrální bankou, která držitele opravňuje poskytovat osobní půjčky nebo působit jako malá finanční organizace.
     - Kopii licence k provozování pikofinančních služeb vydané Ministerstvem financí, která držitele opravňuje působit jako poskytovatel půjček z kategorie Pico nebo Pico-plus.

Příklad běžného porušení zásad:



Hazardní hry, hry a soutěže se skutečnými penězi

Povolujeme hazardní hry se skutečnými penězi, reklamy související s hazardními hrami se skutečnými penězi, věrnostní programy s herními prvky 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 ve vybraných zemích, 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:

- online kasinové hry,
- sportovní sázení,
- sázení na koňské dostihy (v zemích, kde je regulováno a licencováno odděleně od sportovního sázení),
- loterie,
- denní fantasy sporty.

Způsobilé aplikace musí splňovat následující požadavky:

- Aby vývojář mohl distribuovat aplikaci na Google 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 bránit v 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 Google Play.
- 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 aplikaci a nejsou součástí dalších testů her se skutečnými penězi popsaných níže, 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 popsaných 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.

Další testy her se skutečnými penězi

Čas od času můžeme ve vybraných oblastech po omezenou dobu testovat určité typy her se skutečnými penězi. Podrobnosti najdete na této stránce v centru nápovědy. Zkušební verze online her s jeřábem v Japonsku skončila 11. června 2023. Od 12. července 2023 je možné na Google Play celosvětově publikovat online hry s jeřábem – za předpokladu, že splní platné právní předpisy a určité požadavky.

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 (přičemž 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 s benefity, výhodami nebo cenami spojenými s peněžní transakcí splňující určité podmínky 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 odměnami spojenými s peněžní transakcí splňující určité podmínky musí splnit tyto požadavky:
  - V aplikaci musí být zveřejněna oficiální pravidla programu.
  - U programů se systémem odměny založeným na proměnné nebo náhodě: V oficiálních podmínkách programu je třeba uvést 1) metodu výpočtu pravděpodobnosti výhry (u programů s fixní pravděpodobností) a 2) metodu výběru výherce (u ostatních programů).
  - V oficiálních podmínkách 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 podmínkách 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:

- Aplikace a reklama (včetně inzerentů) musí splňovat všechny příslušné právní předpisy a oborové standardy ve všech oblastech, kde se reklama zobrazuje.
- Reklama musí splňovat příslušné místní licenční podmínky pro všechny propagované produkty a služby související s hazardními hrami.
- Aplikace nesmí reklamu na hazardní hru zobrazovat osobám, o kterých je známo, že jsou mladší 18 let.
- Aplikace nesmí být zařazena do programu Pro celou rodinu.
- Aplikace nesmí cílit na osoby mladší 18 let.

- Reklama 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.
- Aplikace nesmí poskytovat simulace obsahu týkajícího se hazardních her (např. aplikace pro kasinové hry pro zábavu, aplikace s virtuálními hracími automaty apod.).
- 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).
- 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 (výše). 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 navržená 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 pro země mimo Spojené státy.
- 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 transakci 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.
- 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 nelegálních drog.
- 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 zahrnují obsah generovaný uživateli (včetně specializovaných prohlížečů a klientů, které přesměrovávají na platformu s takovým obsahem), musí implementovat robustní, efektivní a nepřetržité moderování takového obsahu:

- Musejí zajistit, aby uživatelé obsah mohli vytvářet nebo nahrávat až po přijetí smluvních podmínek nebo zásad pro uživatele aplikace.
- Ve smluvních podmínkách nebo v zásadách pro uživatele aplikace musejí definovat nevhodný obsah a chování (v souladu s programovými zásadami služby Google Play pro vývojáře) a zakázat je.
- Musejí provádět moderování obsahu generovaného uživateli způsobem přiměřeným a odpovídajícím typům obsahu, který je v aplikaci hostován. To zahrnuje poskytnutí systému v aplikaci k nahlašování a blokování nežádoucího obsahu generovaného uživateli a uživatelů a případně také přijímání opatření proti obsahu generovanému uživateli nebo uživatelům. Různá prostředí s obsahem generovaným uživateli mohou vyžadovat různou míru moderování. Příklad:
  - Aplikace s obsahem generovaným uživateli, které identifikují určitou skupinu uživatelů prostřednictvím prostředků, jako je ověření uživatele nebo offline registrace (například aplikace používané výhradně v konkrétní škole nebo společnosti apod.), musí v aplikaci poskytovat funkce k nahlášení obsahu a uživatelů.
  - Funkce s obsahem generovaným uživateli, které umožňují interakci mezi dvěma konkrétními uživateli (například přímé zasílání zpráv, označování, zmínky apod.), musí poskytovat funkce k zablokování uživatelů.
  - Aplikace, které poskytují přístup k veřejně přístupnému obsahu generovanému uživateli, jako jsou aplikace pro sociální sítě a bloggerské aplikace, musí implementovat funkce k nahlašování uživatelů a obsahu a k blokování uživatelů.
  - V případě aplikací s rozšířenou realitou (RR) musí moderování obsahu generovaného uživateli (včetně systému k nahlašování v aplikaci) brát v potaz jak uživateli generovaný nevhodný obsah s RR (například sexuálně explicitní obrázek v RR), tak i ukotvení RR na citlivém místě (například obsah v RR ukotvený v zakázané oblasti, například na vojenské základně nebo na soukromém pozemku, kde by ukotvení v RR mohlo majiteli způsobit problémy).
- Musejí poskytovat bezpečnostní opatření, která zajistí, aby možnosti zpeněžení v aplikaci nepodporovaly nevhodné chování uživatelů.

Vedlejší sexuální obsah

Sexuální obsah je považován za „vedlejší“, pokud se objeví v aplikaci s obsahem generovaným uživateli, která (1) poskytuje přístup primárně k nesexuálnímu obsahu a (2) aktivně nepropaguje ani nedoporučuje sexuální obsah. Sexuální obsah definovaný platnými právními předpisy jako nelegální a obsah ohrožující děti se nepovažují za „vedlejší“ a jsou zakázány.

Aplikace s obsahem generovaným uživateli smí zahrnovat vedlejší sexuální obsah, pokud jsou splněny následující požadavky:

- Takovýto obsah je ve výchozím nastavení skryt filtry, které k deaktivování vyžadují alespoň dvě akce uživatele (například je překrytý vsunutou obrazovkou nebo je jeho zobrazení zablokováno, dokud uživatel nevypne bezpečné vyhledávání).
- Dětem (podle definice v zásadách pro rodiny) je přístup do aplikace blokován systémem pro ověřování věku, jako je neutrální věkový filtr nebo jiný systém definovaný platnými právními předpisy.
- Aplikace poskytuje přesné odpovědi na dotazník ohledně hodnocení obsahu v souvislosti s obsahem generovaným uživateli, jak vyžadují zásady pro hodnocení obsahu.

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.

Obsah a služby zaměřené na zdraví

Nepovolujeme aplikace, které uživatele vystavují zdraví škodlivému obsahu a službám.

Pokud vaše aplikace obsahuje nebo propaguje zdravotní obsah a služby, musíte zajistit, aby byla v souladu s platnými právními předpisy.

Aplikace pro zdraví

Pokud vaše aplikace přistupuje ke zdravotním údajům a buď se jedná o zdravotní aplikaci, nebo nabízí funkce související se zdravím, musí kromě stávajících zásad služby Google Play pro vývojáře, včetně sekcí Ochrana soukromí, ochrana před podvody a zabránění zneužití zařízení a Citlivé události, splňovat také následující požadavky:

- **Deklarace v Play Console:**
  - V Play Console přejděte na stránku Obsah aplikace (Zásady > Obsah aplikace) a vyberte kategorii nebo kategorie, do kterých aplikace patří.
- **Požadavky na zásady ochrany soukromí a oznámení na viditelném místě:**
  - U aplikace musí být v příslušném poli v Play Console uveden odkaz na zásady ochrany soukromí a v aplikaci musí být k dispozici text zásad ochrany soukromí nebo odkaz na ně. Zásady ochrany soukromí musí být k dispozici jako aktivní celosvětově veřejně přístupná adresa URL (ne ve formátu PDF) a nesmí být upravitelné (jak je uvedeno v sekci Zabezpečení údajů).
  - Zásady ochrany soukromí aplikace musí spolu s případnými oznámeními v aplikaci komplexně informovat o tom, jak aplikace načítá, shromažďuje, používá a sdílí osobní nebo citlivé údaje o uživatelích, bez omezení na data uvedená v sekci Zabezpečení údajů výše. U jakýchkoliv funkcí či dat, která jsou regulována pomocí nebezpečných oprávnění nebo oprávnění po spuštění , musí aplikace splnit všechny příslušné požadavky na souhlas a oznámení na viditelném místě.
  - Zdravotní aplikace nesmí žádat o oprávnění, která nepotřebuje k vykonávání své hlavní funkce, a nepoužívaná oprávnění je potřeba odstranit. Seznam oprávnění, která jsou považována za oprávnění spojená s citlivými údaji souvisejícími se zdravím, najdete v článku Kategorie zdravotních aplikací a další informace.
  - Zásady pro zdravotní aplikace se vztahují i na aplikace, které nejsou primárně zdravotními aplikacemi, ale mají funkce související se zdravím a mají přístup ke zdravotním údajům. Spojení

mezi hlavní funkcí aplikace a shromažďováním údajů souvisejících se zdravím by uživateli mělo být jasné (jako například u poskytovatelů pojištění, herních aplikací, které shromažďují údaje o aktivitě uživatele jako způsob postupu ve hře, a podobně). Zásady ochrany soukromí aplikace musí odrážet toto omezené využití.

- **Další požadavky:**
  Pokud vaše zdravotní aplikace odpovídá některému z následujících označení, musíte kromě výběru příslušné kategorie v Play Console splňovat také příslušné požadavky:
  - **Zdravotní aplikace spojené s veřejnoprávními subjekty:** Pokud máte od veřejnoprávního subjektu nebo uznávané zdravotnické organizace povolení vyvíjet a distribuovat aplikaci spojenou s tímto subjektem, musíte odeslat doklad o způsobilosti prostřednictvím formuláře předběžného oznámení.
  - **Aplikace ke sledování kontaktů či zdravotního stavu:** Pokud je vaše aplikace aplikací pro sledování kontaktů a/nebo zdravotního stavu, vyberte v Play Console možnost Prevence onemocnění a veřejné zdraví a pomocí formuláře předběžného oznámení výše poskytněte požadované informace.
  - **Aplikace pro výzkum lidských subjektů:** Aplikace provádějící výzkum týkající se lidského zdraví musí splňovat všechna pravidla a předpisy, mimo jiné včetně získání informovaného souhlasu od účastníků nebo, v případě nezletilých, jejich rodiče nebo zákonného zástupce. Aplikace pro zdravotní výzkum také musejí mít schválení od institucionální kontrolní komise a/nebo nezávislé etické komise (pokud se na ně nevztahuje výjimka). Na požádání je nutné předložit doklad o takovémto schválení.
  - **Aplikace považované za lékařská zařízení nebo za software plnící funkci lékařského zařízení:** Aplikace, které jsou považovány za lékařská zařízení nebo za software plnící funkci lékařského zařízení, musí získat a uchovat si potvrzení o schválení nebo jinou schvalovací dokumentaci poskytnutou regulačním úřadem nebo orgánem odpovědným za správu a shodu zdravotní aplikace. Na požádání je nutné předložit doklad o takovémto povolení nebo schválení.

Údaje služby Health Connect

Údaje přístupné na základě oprávnění Health Connect jsou považovány za osobní a citlivé údaje o uživateli, na které se vztahují zásady pro údaje o uživatelích a další požadavky .

Léky na předpis

Nepovolujeme aplikace, které umožňují prodej nebo nákup léků na předpis bez lékařského předpisu.

Neschválené látky

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

Příklady běžných porušení zásad:

- 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 neschválených či zavádějících léčivech a doplňcích, které sledujeme, naleznete na webu www.legitscript.com .

Dezinformace o zdraví

Nepovolujeme aplikace obsahující zavádějící zdravotní tvrzení, která jsou v rozporu se stávajícím lékařským konsensem nebo mohou poškodit uživatele.

Příklady běžných porušení zásad:

- Zavádějící tvrzení o vakcínách, například že vakcíny mohou lidem změnit DNA.
- Obhajoba škodlivé, neschválené léčby.
- Prosazování jiných škodlivých zdravotních praktik, jako je konverzní terapie.

Lékařské funkce

Nepovolujeme aplikace s lékařskými nebo zdravotnickými funkcemi, které mohou poskytovat nesprávné informace nebo uživateli potenciálně uškodit. Nepovolujeme například aplikace, které tvrdí, že mají funkci oxymetrie založenou ryze na aplikaci. Oxymetrické aplikace vyžadují externí hardware, nositelné zařízení nebo speciální senzory na telefonu. Podporované aplikace tohoto typu navíc musí v metadatech uvádět odmítnutí odpovědnosti, že nejsou určeny pro lékařské použití a že se nejedná ani o lékařské zařízení, ale že jsou určeny pouze pro obecné sledování kondice a zdravotního stavu. Musí také uvádět kompatibilní model hardwaru/zařízení.

Platby – klinické služby

Transakce týkající se regulovaných klinických služeb nesmí využívat fakturační systém Google Play. Další informace naleznete v článku zásady služby Google Play pro platby .

Obsah vycházející z blockchainu

Blockchainové technologie se rychle rozvíjejí, proto se snažíme vývojářům poskytnout platformu, která bude těžit z inovací a bude uživatelům nabízet široké možnosti.

Pro účely těchto zásad považujeme blockchainový obsah za tokenizované digitální položky zabezpečené pomocí blockchainu. Pokud vaše aplikace zahrnuje blockchainový obsah, je nutné dodržovat tyto požadavky.

Burzy kryptoměn a softwarové peněženky na kryptoměny

Nákup, držení a výměna kryptoměn musí v regulovaných jurisdikcích probíhat prostřednictvím certifikovaných služeb.

Je také nutné dodržovat platné regulace v zemích/oblastech, na které vaše aplikace cílí, a nesmíte ji publikovat tam, kde jsou vaše produkty a služby zakázány. Google Play může požadovat poskytnutí dalších informací nebo dokumentů, které potvrzují, že dodržujete regulační nebo licenční podmínky.

Těžba kryptoměn

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

Požadavky na transparentnost v souvislosti s distribucí tokenizovaných digitálních položek

Pokud vaše aplikace prodává nebo umožňuje získání tokenizovaných digitálních položek, musíte to deklarovat v Play Console na stránce Obsah aplikace pomocí formuláře Finanční funkce.

Při vytváření produktu v aplikaci je nutné v jeho podrobnostech uvést, že se jedná o tokenizovanou digitální položku. Další pokyny najdete v článku Vytvoření produktu v aplikaci.

Není dovoleno propagovat nebo vychvalovat potenciální zisk z hraní nebo výměny.

Další požadavky na gamifikaci NFT

Zásady her, soutěží a hazardních her se skutečnými penězi na Google Play vyžadují, aby hazardní aplikace s tokenizovanými digitálními položkami (jako jsou NFT) dokončily proces žádosti.

U všech ostatních aplikací, které nesplňují výše uvedené požadavky na způsobilost hazardních aplikaci a nejsou součástí dalších testů her se skutečnými penězi, není dovoleno provádět výměny peněžní hodnoty za šanci na získání NFT s neznámou hodnotou. NFT zakoupené uživateli musí být využity ve hře ke zlepšení uživatelského zážitku nebo k usnadnění postupu hrou. NFT nesmí být využity k sázení na příležitost získat ceny s peněžní hodnotou v reálném světě (včetně dalších NFT).

Příklady běžných porušení zásad:

- Aplikace, které prodávají balíčky NFT bez uvedení konkrétního obsahu a hodnoty NFT
- Placené kasinové hry pro zábavu (např. výherní automaty), které umožňují vyhrát NFT

Obsah generovaný umělou inteligencí

S tím, jak jsou modely generativní umělé inteligence pro vývojáře stále dostupnější, můžete tyto modely začleňovat do svých aplikací, abyste zvýšili zapojení a zlepšili uživatelský dojem. Google Play chce pomoci zajistit, aby byl obsah generovaný umělou inteligencí bezpečný pro všechny uživatele a aby byla zohledňována zpětná vazba od uživatelů, která umožní odpovědné inovace.

Obsah generovaný umělou inteligencí

Obsah generovaný umělou inteligencí je obsah, který na základě pokynů uživatelů vytvářejí modely generativní umělé inteligence. Příklady obsahu generovaného umělou inteligencí:

- Konverzační generativní chatboty využívající generativní umělou inteligenci, ve kterých je interakce s chatbotem ústřední funkcí aplikace
- Obrázek vygenerovaný umělou inteligencí na základě textu, obrázku nebo hlasových pokynů

Aby byla zajištěna bezpečnost uživatelů a v souladu s rozsahem zásad služby Google Play musejí aplikace, které generují obsah pomocí umělé inteligence, dodržovat stávající zásady služby Google Play pro vývojáře, včetně zákazu a zabránění generování omezeného obsahu, jako je například obsah umožňující využívání nebo obtěžování dětí a obsah umožňující klamavé chování.

Aplikace, které generují obsah pomocí umělé inteligence, musí obsahovat funkce, pomocí nichž mohou uživatelé vývojářům nahlásit urážlivý obsah, aniž by aplikaci museli opustit. Vývojáři by uživatelská hlášení měli používat k filtrování a moderování obsahu v aplikacích.

Duševní vlastnictví

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

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

Chcete-li podat stížnost na prodej nebo propagaci prodeje padělaného zboží v aplikaci, odešlete oznámení o padělání .

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

Pokud máte písemné potvrzení, že v aplikaci nebo záznamu v obchodu smíte použít duševní vlastnictví třetí strany (např. název a logo značky, grafické podklady apod.), před odesláním aplikace kontaktujte tým podpory Google Play , aby bylo zajištěno, že aplikace nebude zamítnuta z důvodu porušení duševního vlastnictví.

Neoprávněné použití obsahu chráněného autorskými právy

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

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

Příklady běžných porušení zásad:

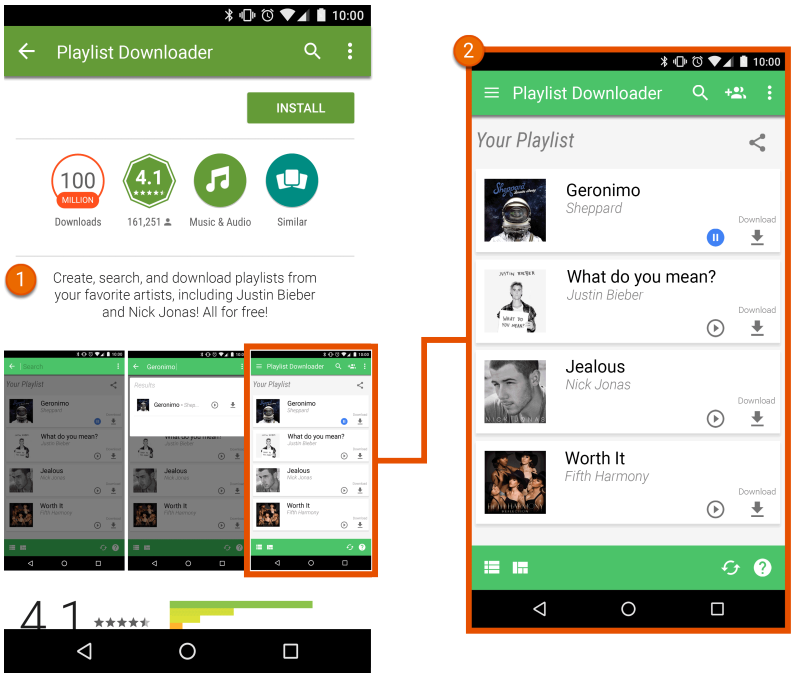
- Obálka hudebního alba, videohry nebo knihy.
- Marketingové obrázky z filmů, televize nebo videoher.
- Díla nebo obrázky z komiksů, kreslených seriálů, filmů, hudebních videí nebo televize.
- Loga vysokých škol a profesionálních sportovních týmů.
- Fotografie pořízené z účtu veřejně známé osobnosti na sociálních médiích.
- Profesionální snímky veřejně známých osobností.
- Reprodukce nebo „fan art“, které nelze odlišit od původního díla chráněného autorskými právy.
- Aplikace se zvukovou klávesnicí, která přehrává zvukové klipy z obsahu chráněného autorskými právy.
- Úplné reprodukce nebo překlady knih, které se nenacházejí ve veřejném vlastnictví.

Podpora porušování autorských práv

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

Příklady běžných porušení zásad:

- Streamovací aplikace, které uživatelům umožňují stáhnout místní kopii obsahu chráněného autorskými právy bez potřebného povolení.
- Aplikace, které uživatele vybízejí ke streamování a stahování děl chráněných autorskými právy (včetně hudby a videí) způsobem, při kterém dochází k porušení autorských práv:



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

Porušení ochranné známky

Nepovolujeme aplikace, které porušují ochranné známky třetích stran. Ochranná známka je slovo, symbol nebo jejich kombinace, která označuje původ produktu nebo služby. Po přidělení poskytuje ochranná známka svému vlastníkovi 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 zneužití sítě, zařízení nebo osobních údajů, jsou přísně zakázány.

Uživatelská data

Musíte být transparentní ohledně toho, jak zacházíte s údaji o uživatelích (například s informacemi, které jste o nich a jeho zařízeních shromáždili). To znamená, že musíte zveřejňovat informace o přístupu, shromažďování, využívání, sdílení údajů o uživatelích z vaší aplikace a nakládání s nimi

a také musíte omezit využití údajů na účely, které jsou v souladu se zásadami a o nichž uživatele informujete. Upozorňujeme, že na nakládání s osobními a citlivými údaji o uživatelích se vztahují také dodatečné podmínky uvedené níže v sekci Osobní a citlivé údaje o uživatelích. Tyto požadavky služby Google Play platí nad rámec povinností, které vyplývají z platných právních předpisů na ochranu soukromí a osobních údajů.

Pokud do aplikace zahrnete kód třetí strany (například sady SDK), musíte zajistit, aby tento kód a postupy této třetí strany ve vztahu k údajům o uživatelích z vaší aplikace neporušovaly programové zásady pro vývojáře Google Play, které zahrnují požadavky na používání a zveřejněné informace. Musíte například zajistit, aby vaši poskytovatelé sad SDK neprodávali osobní a citlivé údaje o uživatelích z vaší aplikace. Tento požadavek platí bez ohledu na to, zda jsou údaje o uživatelích přenášeny po odeslání na server nebo prostřednictvím vložení kódu třetí strany do vaší aplikace.

Osobní a citlivé údaje o uživateli

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, zdravotní údaje , údaje z aplikace Health Connect , inventář ostatních aplikací v zařízení, údaje z mikrofonu a fotoaparátu a jiné citlivé údaje o zařízení a jeho využití. Pokud vaše aplikace zpracovává osobní a citlivé uživatelské údaje, musíte dodržet tyto pokyny:

- Shromažďování, využívání a sdílení osobních a citlivých údajů získaných prostřednictvím aplikace musíte omezit na funkce aplikace a služeb a účely související s dodržováním zásad, které jsou v souladu s přiměřeným očekáváním uživatelů:
  - Aplikace, které využívají osobní a citlivé údaje o uživatelích k zobrazování reklam, musí splňovat zásady inzerce služby Google Play.
  - Údaje můžete v případě potřeby přenést k poskytovatelům služeb nebo z právních důvodů, například ke splnění platných žádostí orgánů státní správy nebo příslušných právních předpisů, či v rámci sloučení nebo akvizice, přičemž je třeba o tom uživatele právně přiměřeným způsobem informovat.
- Všechny osobní a citlivé údaje o uživatelích musíte zpracovávat zabezpečeným způsobem včetně přenosu šifrovaného moderními metodami (např. pomocí protokolu HTTPS).
- Pokud je to možné, před přístupem k údajům pomocí oprávnění systému Android používejte žádost o oprávnění po spuštění.
- Osobní a citlivé údaje o uživatelích nesmíte prodávat.
  - „Prodej“ znamená výměnu nebo přenos osobních a citlivých údajů o uživatelích třetí straně za peněžní úplatu.
    - Za prodej není považován přenos osobních a citlivých údajů iniciovaný uživatelem (například když uživatel pomocí funkce aplikace přenáší soubor třetí straně, nebo když se uživatel rozhodne použít speciální aplikaci pro výzkumnou studii).

Požadavky na oznámení na viditelném místě a souhlas

V případě, kdy vaše aplikace shromažďuje, používá či sdílí osobní a citlivé údaje o uživatelích nebo k nim přistupuje, a tato činnost není v souladu s přiměřeným očekáváním uživatele příslušné služby nebo funkce (například pokud shromažďování údajů probíhá na pozadí, když uživatel s aplikací nepracuje), musíte splnit následující požadavky:

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

- Musí být přímo v aplikaci, nikoli pouze v popisu aplikace či na webu.
- Musí se zobrazovat při běžném používání aplikace a nesmí vyžadovat, aby uživatel přešel do nabídky nebo nastavení.
- Musí popisovat, jaká data se používají nebo shromažďují.
- Musí vysvětlovat, jakým způsobem budou data využita či sdílena.

- Nesmí být umístěno pouze v zásadách ochrany soukromí nebo smluvních podmínkách.
- Nesmí být zahrnuto mezi ostatními oznámeními, která se netýkají shromažďování osobních a citlivých údajů o uživatelích.

Souhlas a oprávnění po spuštění: Žádostem o souhlas uživatele v aplikaci a žádostem o oprávnění po spuštění musí bezprostředně předcházet oznámení v aplikaci, které splňuje požadavek těchto zásad. 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 (například 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 zavřou (např. po vypršení časového limitu).
- Uživatel musí souhlas udělit dříve, než aplikace začne shromažďovat osobní a citlivé údaje o uživateli nebo k nim přistupovat.

Aplikace, které zpracovávají osobní a citlivé údaje o uživatelích bez souhlasu na základě jiných právních základů, jako je například oprávněný zájem podle nařízení GDPR Evropské unie, musí splňovat všechny příslušné právní podmínky a zobrazovat uživatelům příslušná oznámení, včetně oznámení v aplikaci požadovaných v rámci těchto zásad.

Pokud je vyžadováno oznámení na viditelném místě, kvůli splnění požadavků stanovených v zásadách doporučujeme řídit se následujícím vzorovým formátem:

- „[Tato aplikace] shromažďuje/přenáší/synchronizuje/ukládá [typ dat], které využívá k poskytování [této funkce] [v jaké situaci].“
- *Příklad: „Aplikace Fitness Funds shromažďuje údaje o poloze, které využívá ke sledování sportovní aktivity, a to i když je zavřená nebo zrovna není používána. Tyto údaje využívá také k inzerci.“*
- *Příklad: „Aplikace Call Buddy shromažďuje údaje ze seznamu hovorů, které využívá k uspořádání kontaktů, a to i v době, kdy není používána.“*

Pokud aplikace obsahuje kód třetí strany (například sady SDK), který je určen k automatickému shromažďování osobních a citlivých údajů o uživatelích, musíte do dvou týdnů od přijetí žádosti od Google Play (nebo v rámci delšího časového období uvedeného v žádosti služby Google Play) poskytnout dostatečný důkaz prokazující, že aplikace splňuje požadavky těchto zásad na viditelné oznámení a souhlas, včetně požadavků na shromažďování, používání a sdílení údajů prostřednictvím kódu třetí strany nebo přistupování k nim.

Příklady běžných porušení zásad:

- Aplikace shromažďuje údaje o poloze zařízení, ale nemá oznámení na viditelném místě s vysvětlením, která funkce tyto údaje využívá nebo že k využívání dochází na pozadí.
- Aplikace zobrazuje oprávnění po spuštění se žádostí o přístup k údajům dříve než oznámení na viditelném místě s vysvětlením účelu shromažďování údajů.
- 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 využívá 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.
- Aplikace se sadou SDK, která shromažďuje osobní a citlivé údaje o uživatelích a nezachází s těmito údaji jako s údaji podléhajícími těmto zásadám pro údaje o uživatelích, včetně přístupu k údajům, nakládání s údaji (včetně nepovoleného prodeje) a požadavků na viditelné oznámení a souhlas.

Další informace o požadavcích na viditelné oznámení a souhlas naleznete v tomto článku.

Omezení přístupu k osobním a citlivým údajům o uživatelích

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.
Vaše aplikace cílí na děti	Aplikace nesmí obsahovat sadu SDK, která není schválena pro služby určené dětem. Úplné znění a požadavky zásad naleznete v článku Navrhování aplikací pro děti a rodiny .
Aplikace shromažďuje nebo odkazuje na trvalé identifikátory zařízení (např. IMEI, IMSI, sériové číslo SIM karty apod.)	Trvalé identifikátory zařízení nesmí být propojeny s jinými osobními a citlivými údaji o uživatelích ani resetovatelnými identifikátory zařízení pro účely: • telefonických služeb spojených s identitou SIM karty (např. volání přes Wi-Fi spojené s účtem u operátora), • podnikových aplikací pro správu zařízení, které využívají režim vlastníka zařízení. Tyto způsoby využití musí být uživatelům viditelně oznámeny, jak je uvedeno v zásadách pro údaje o uživatelích . Alternativní unikátní identifikátory jsou popsány zde . Další pokyny v souvislosti s inzertním ID Android naleznete v zásadách inzerce .

Sekce Zabezpečení údajů

Každý vývojář musí u každé své aplikace vyplnit sekci Zabezpečení údajů, ve které popíše shromažďování, využití a předávání údajů o uživatelích. Vývojář ručí za přesnost a aktuálnost štítku a uvedených informací. Pokud je to relevantní, údaje v sekci musí být v souladu s oznámeními v zásadách ochrany soukromí aplikace.

Další informace o vyplnění sekce Zabezpečení údajů najdete v tomto článku .

Zásady ochrany soukromí

U všech aplikací musí být v označeném poli v Play Console uveden odkaz na zásady ochrany soukromí. U všech aplikací musí být text zásad ochrany soukromí nebo odkaz na ně zveřejněn také v samotné aplikaci. Zásady ochrany soukromí společně s případnými oznámeními v aplikaci musí jasně popisovat,

jak aplikace načítá, shromažďuje, využívá a sdílí údaje o uživatelích, a to nad rámec údajů uvedených v sekci Zabezpečení údajů. Musí být uvedeny následující informace:

- údaje o vývojáři, kontakt pro účely ochrany soukromí nebo mechanismus k odesílání dotazů,
- typy osobních a citlivých údajů o uživatelích, které aplikace načítá, shromažďuje, používá a sdílí, a informace o tom, kterým třetím stranám je poskytuje,
- zabezpečené procesy nakládání s údaji,
- zásady vývojáře pro uchovávání a mazání dat,
- jasné označení, že se jedná o zásady ochrany soukromí (například název sekce „Zásady ochrany soukromí“).

V zásadách ochrany soukromí musí být uveden subjekt (tj. vývojář, společnost) uvedený v záznamu aplikace v obchodě Google Play nebo název aplikace. Zásady ochrany soukromí musí mít i aplikace, které nenačítají žádné osobní ani citlivé údaje o uživatelích.

Zásady ochrany soukromí musí být k dispozici jako aktivní celosvětově veřejně přístupná adresa URL (ne ve formátu PDF) a nesmí být upravitelné.

Požadavek na smazání účtu

Pokud uživatelé ve vaší aplikaci mohou vytvářet účty, musí mít možnost je také smazat. Uživatelé musí mít snadno objevitelnou možnost smazat svůj účet přímo v aplikaci nebo mimo ni (např. na vašem webu). Odkaz na tento webový zdroj je nutné zadat do určeného pole pro adresu URL ve formuláři v Play Console.

Když na žádost uživatele smažete účet pro aplikaci, musíte smazat i uživatelská data spojená s daným účtem. Za smazání se nepovažuje dočasná deaktivace nebo „zmrazení“ účtu. Pokud z legitimních důvodů, jako je bezpečnost, předcházení podvodům nebo dodržování předpisů, určitá data potřebujete uchovat, musíte uživatele informovat o svých postupech uchovávání dat (např. v rámci zásad ochrany soukromí).

Další informace o požadavcích zásad ohledně smazání účtu najdete v tomto článku centra nápovědy. Další informace o aktualizaci formuláře Zabezpečení údajů najdete v tomto článku.

Použití ID nastaveného aplikací

V Androidu bude zavedeno nové ID, které bude podporovat základní případy použití, jako je analýza a prevence podvodů. Podmínky využití tohoto identifikátoru jsou uvedeny níže.

- **Použití:** ID nastavené aplikací nesmí sloužit k personalizaci nebo měření reklam.
- **Spojení s údaji umožňujícími zjištění totožnosti nebo jinými identifikátory:** ID nastavené aplikací nesmí být spojeno s jinými identifikátory na platformě Android ani se žádnými osobními nebo citlivými údaji pro účely inzerce.
- **Transparentnost a souhlas:** Uživatelé musejí být o shromažďování a využití ID nastaveného aplikací a závazku dodržovat tyto smluvní podmínky informováni v právně přiměřené formě oznámení o ochraně soukromí, které musí zahrnovat vaše zásady ochrany soukromí. Od koncových uživatelů musíte ve vyžadovaných případech získat právně platný souhlas. Další informace o standardech ochrany soukromí naleznete v zásadách používání údajů o uživatelích .

EU-U.S. a Swiss-U.S. Privacy Shield (štít soukromí)

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.

Od 16. července 2020 už společnost Google při předávání osobních údajů pocházejících z Evropského hospodářského prostoru nebo Spojeného království do USA nespoléhá na EU-U.S. Privacy Shield. (Další informace) Další informace naleznete v sekci 9 distribuční smlouvy pro vývojáře.

Oprávnění a rozhraní API s přístupem k citlivým údajům

Žádosti o oprávnění a rozhraní API, která mají přístup k citlivým údajům, musí uživatelům dávat smysl. Můžete žádat pouze o oprávnění a rozhraní API s přístupem k citlivým údajům, která jsou nezbytná k implementaci existujících funkcí nebo služeb v aplikaci, které propagujete v záznamu na Google Play. Nesmíte používat oprávnění nebo rozhraní API s přístupem k citlivým údajům, která umožňují přístup k údajům o uživateli nebo zařízení za účelem využití v neuvedených, neimplementovaných nebo nedovolených funkcích. Osobní a citlivé údaje získané prostřednictvím oprávnění nebo rozhraní API s přístupem k citlivým údajům je zakázáno prodávat nebo sdílet za účelem zprostředkování prodeje.

O přístup k údajům prostřednictvím oprávnění a rozhraní API s přístupem k citlivým údajům se snažte žádat co nejvíce v kontextu (prostřednictvím inkrementálních žádostí), 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 rozdělena na Nebezpečná , Zvláštní nebo Podpisová nebo jak je uvedeno níže. Na tato oprávnění se vztahují následující dodatečné požadavky a omezení:

- Údaje o uživatelích nebo zařízeních získané prostřednictvím omezených oprávnění jsou považovány za osobní a citlivé údaje o uživatelích. Vztahují se na ně zásady pro údaje o uživatelích .
- 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 (například umožnit ruční zadání telefonního čísla, pokud uživatel odmítne přístup k seznamu hovorů).
- Používání oprávnění v rozporu se zásadami Google Play ohledně malwaru (včetně zneužití zvýšených oprávnění) je výslovně zakázáno.

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 bezpečnost uživatelů.

Oprávnění k přístupu k SMS a seznamu hovorů

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

Omezené oprávnění	Požadavek
Skupina oprávnění Seznam hovorů (např. READ_CALL_LOG, WRITE_CALL_LOG, PROCESS_OUTGOING_CALLS)	Musí být v zařízení aktivně zaregistrován jako výchozí obslužný nástroj typu Telefon nebo Asistence.
Skupina oprávnění SMS (např. READ_SMS, SEND_SMS, WRITE_SMS, RECEIVE_SMS, RECEIVE_WAP_PUSH, RECEIVE_MMS)	Musí být v zařízení aktivně zaregistrován jako výchozí obslužný nástroj typu SMS nebo Asistence.

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

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

Oprávnění pro přístup k poloze

Poloha zařízení je považována za osobní a citlivý údaj o uživateli a vztahují se na ni zásady uvedené v sekci Osobní a citlivé údaje , zásady pro používání polohy na pozadí 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 .

Další informace o požadavcích zásad najdete v tomto článku nápovědy .

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 nebo novější budou vyžadovat svolení 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 .

Oprávnění viditelnosti balíčku (aplikace)

Inventář nainstalovaných aplikací vyžádaných ze zařízení je považován za osobní a citlivý údaj o uživatelích. Vztahují se na něj zásady uvedené v sekci Osobní a citlivé údaje a také následující požadavky:

Aplikace, jejichž hlavním účelem je spuštění, vyhledávání nebo spolupráce s jinými aplikacemi v zařízení, mohou v náležitém rozsahu zjistit ostatní aplikace nainstalované v zařízení, jak je uvedeno níže:

- **Obecná viditelnost aplikací:** Obecná viditelnost je schopnost aplikace zjistit nainstalované aplikace („balíčky“) v zařízení v rozsáhlém („obecném“) měřítku.
  - V případě aplikací, které cílí na úroveň rozhraní API 30 nebo novější , je obecná viditelnost nainstalovaných aplikací dosažená prostřednictvím oprávnění QUERY_ALL_PACKAGES omezena na konkrétní případy užití, kdy je k fungování aplikace potřeba, aby aplikace znala všechny ostatní aplikace v zařízení nebo s nimi komunikovala.
    - Oprávnění QUERY_ALL_PACKAGES nesmíte použít, pokud aplikace může fungovat s více zacílenou deklarací rozsahu viditelnosti balíčku (např. dotazy na konkrétní balíčky a interakce s nimi namísto požadování obecné viditelnosti).
  - Omezení se vztahují také na alternativní metody, kterými je možné přiblížit se k úrovni obecné viditelnosti, kterou poskytuje oprávnění QUERY_ALL_PACKAGES. Tyto metody lze použít výhradně k poskytování základní funkce aplikace pro uživatele a v případě, že bude zajištěna spolupráce s ostatními aplikacemi objevenými touto metodou.
  - Informace o povolených případech užití oprávnění QUERY_ALL_PACKAGES naleznete v tomto článku centra nápovědy .
- **Omezená viditelnost aplikací**: Omezená viditelnost nastává, když aplikace minimalizuje přístup k datům tím, že odešle dotazy na konkrétní aplikace pomocí více zacílených (tedy ne „obecných“) metod (např. dotazy na konkrétní aplikace, které vyhovují deklaraci manifestu aplikace). Pomocí této metody můžete odesílat dotazy na aplikace v případech, kdy aplikace umožňuje spolupráci s těmito aplikacemi nebo správu těchto aplikací v souladu se zásadami.
- Viditelnost inventáře aplikací nainstalovaných v zařízení musí přímo souviset s hlavním účelem nebo hlavní funkcí, kterou uživatelé v aplikaci využívají.

Data o inventáři aplikací získaná z aplikací distribuovaných ve službě Play nesmí být prodávána ani sdílena pro účely analýzy nebo zpeněžování reklam.

Rozhraní API pro přístupnost

Použití rozhraní API pro přístupnost má následující omezení:

- Nesmí bez souhlasu uživatele měnit nastavení ani bránit uživatelům v deaktivování nebo odinstalaci jakékoli aplikace nebo služby, kromě případů, kdy to povolí rodič nebo zákonný zástupce prostřednictvím aplikace rodičovské kontroly nebo administrátor prostřednictvím softwaru na správu podniku.

- Nesmí obcházet nastavení ochrany soukromí a oznámení systému Android.
- Nesmí měnit ani zneužívat uživatelské rozhraní způsobem, který je klamavý nebo jiným způsobem porušuje zásady pro vývojáře Google Play.

Rozhraní Accessibility API není určeno ke vzdálenému nahrávání hovorů a nemůže být k tomuto účelu požadováno.

Použití rozhraní API pro přístupnost musí být zdokumentováno v záznamu na Google Play.

Pokyny pro příznak IsAccessibilityTool

Aplikace, jejichž hlavní funkcí je přímá podpora uživatelů s postižením, smí používat příznak **IsAccessibilityTool** k veřejnému označení, že se jedná o aplikaci k usnadnění přístupu.

Aplikace, které pro příznak **IsAccessibilityTool** nejsou způsobilé, toto označení používat nesmí a musí splňovat pravidla pro jasné zveřejnění a souhlas popsaná v zásadách nakládání s údaji o uživatelích, protože funkce související s přístupností nejsou pro uživatele zřejmé. Další informace naleznete v článku centra nápovědy o rozhraní AccessibilityService API.

Aplikace musí namísto rozhraní Accessibility API k dosažení požadovaných funkci používat rozhraní API a oprávnění s užším rozsahem.

Oprávnění žádat o instalaci balíčků

Oprávnění REQUEST_INSTALL_PACKAGES umožňuje aplikaci žádat o instalaci balíčků aplikace. Hlavní funkce aplikace, která může toto oprávnění využívat, musí zahrnovat:

- odesílání nebo příjem balíčků aplikace,
- povolení instalace balíčků aplikace iniciované uživatelem.

Povolené funkce zahrnují:

- procházení internetu nebo vyhledávání,
- komunikační služby podporující přílohy,
- sdílení, převádění a stahování souborů,
- podniková správa zařízení,
- zálohování a obnovení,
- migrace zařízení / přenos telefonu,
- doprovodná aplikace k synchronizaci telefonu s nositelným zařízením nebo internetem věcí (např. chytrými hodinkami nebo televizí).

Hlavní funkce je základním účelem aplikace. Hlavní funkce (včetně dílčích funkcí, které jsou součástí základní funkčnosti) je taková, která je nejvýrazněji zdokumentována a propagována v popisu aplikace.

Oprávnění REQUEST_INSTALL_PACKAGES se nesmí používat k aktualizacím, úpravám nebo seskupování jiných balíčků APK v souboru podkladu, pokud se nejedná o akci v rámci správy zařízení. Všechny aktualizace a instalace balíčků musí dodržovat zásady Google Play ohledně zneužívání zařízení a sítě a musí to být uživatel, kdo je zahájí a má pod kontrolou.

Oprávnění Health Connect by Android

Health Connect je platforma Android, která umožňuje aplikacím pro zdraví a fitness ukládat a sdílet data tohoto typu v zařízení v rámci jednotného ekosystému. Nabízí také uživatelům jednotné místo k ovládání, které aplikace mohou číst a zapisovat údaje o zdraví a kondici. Health Connect podporuje čtení a zápis různých typů dat, od kroků po tělesnou teplotu.

Údaje přístupné na základě oprávnění Health Connect jsou považovány za osobní a citlivé údaje o uživateli, na které se vztahují zásady pro údaje o uživatelích. Pokud je vaše aplikace považována za zdravotní aplikaci nebo má funkce související se zdravím a přistupuje ke zdravotním údajům, včetně údajů aplikace Health Connect, musí splňovat také zásady pro zdravotní aplikace.

Informace o tom, jak s aplikací Health Connect začít, najdete v tomto průvodci pro vývojáře aplikací pro Android . Pokud chcete požádat o přístup k typům dat aplikace Health Connect, přečtěte si tento článek.

Aplikace distribuované prostřednictvím Google Play musí splňovat následující zásady, aby mohly číst a/nebo zapisovat data do Health Connect.

Náležitý přístup ke službě Health Connect a její používání

Platformu Health Connect je dovoleno používat pouze v souladu s příslušnými zásadami, podmínkami a pro schválené případy použití, jak je uvedeno v těchto zásadách. To znamená, že o přístup k oprávněním můžete požádat pouze v případě, že vaše aplikace nebo služba splňuje některý ze schválených případů použití.

Mezi schválené případy použití patří: fitness a kvalita života, odměny, fitness koučování, firemní zdraví, lékařská péče, zdravotní výzkum a hry. Aplikace, které tato oprávnění získají, je nesmí používat k nezveřejněným nebo nepovoleným účelům.

O přístup k oprávněním Health Connect smějí žádat pouze aplikace nebo služby s jednou nebo více funkcemi, jejichž primárním účelem je podporovat zdraví a kondici uživatelů. Patří mezi ně:

- aplikace nebo služby, které uživatelům umožňují přímo **zaznamenávat, hlásit, sledovat a/nebo analyzovat** fyzickou aktivitu, spánek, duševní pohodu, výživu, zdravotní měření, popisy fyzických vlastností a/nebo jiné popisy a měření týkající se zdraví či kondice,
- aplikace nebo služby, které uživatelům umožňují **ukládat do telefonu a/nebo nositelného zařízení informace o fyzické aktivitě, spánku, duševní pohodě, výživě či zdravotních měřeních, popisy tělesné kondice** a/nebo jiné popisy a měření týkající se zdraví nebo fyzické kondice a sdílet tyto údaje s jinými aplikacemi v zařízení, které splňují tyto případy použití.

Přístup k platformě Health Connect nesmí být používán v rozporu s těmito zásadami nebo jinými platnými smluvními podmínkami nebo zásadami platformy Health Connect, a to ani k následujícím účelům:

- Nepoužívejte Health Connect při vývoji nebo k začlenění do aplikací, prostředí či aktivit, u nichž lze důvodně očekávat, že by použití nebo selhání platformy Health Connect mohlo vést k úmrtí, zranění osob nebo poškození životního prostředí či majetku (například při vytváření nebo provozu jaderných zařízení, řízení letového provozu, systémů podpory života nebo zbraní).
- Nepřistupujte k údajům získaným prostřednictvím platformy Health Connect pomocí aplikací bez grafické vrstvy. Aplikace musí mít jasně identifikovatelnou ikonu na liště aplikací, v nastavení aplikací v zařízení, na ikonách oznámení apod.
- Nepoužívejte Health Connect s aplikacemi, které synchronizují data mezi nekompatibilními zařízeními nebo platformami.
- Nepoužívejte Health Connect k připojení k aplikacím, službám nebo funkcím, které jsou zaměřeny výhradně na děti.
- Přijměte přiměřená a vhodná opatření k ochraně všech aplikací nebo systémů, které využívají Health Connect, před neoprávněným nebo nezákonným přístupem, použitím, zničením, ztrátou, změnou nebo zveřejněním.

Je také vaší odpovědností zajistit soulad s veškerými regulačními nebo právními požadavky, které se na vás na základě zamýšleného použití platformy Health Connect a jakýchkoliv údajů z ní mohou vztahovat. S výjimkou případů, kdy je to výslovně uvedeno v označení nebo informacích poskytovaných společností Google pro konkrétní produkty nebo služby Google, společnost Google neschvaluje použití ani nezaručuje přesnost jakýchkoliv údajů obsažených v Health Connect pro jakékoliv účely, zejména pro výzkumné, zdravotní či lékařské účely. Společnost Google se zříká veškeré odpovědnosti spojené s použitím dat získaných prostřednictvím platformy Health Connect.

Omezené použití

Při používání aplikace Health Connect musí přístup k datům a jejich používání splňovat konkrétní omezení:

- Použití dat musí být omezeno na poskytování nebo vylepšování náležitého případu použití nebo funkcí viditelných v uživatelském rozhraní aplikace.
- Údaje o uživatelích mohou být předány třetím stranám pouze s výslovným souhlasem uživatele: z bezpečnostních důvodů (například k vyšetřování zneužití), k zajištění souladu s platnými zákony nebo předpisy, případně v rámci fúzí/akvizic.
- Lidé smí mít k údajům o uživatelích přístup, pouze pokud to uživatel výslovně povolil, pokud je to vyžadováno z bezpečnostních důvodů nebo pokud se jedná o využití souhrnných dat k interním účelům v souladu s právními požadavky.
- Veškeré jiné přenosy, použití nebo prodeje údajů aplikace Health Connect jsou zakázány, a to včetně těchto:
  - přenos nebo prodej údajů o uživatelích třetím stranám, jako jsou reklamní platformy, zprostředkovatelé dat nebo přeprodejci informací,
  - přenos, prodej nebo používání údajů o uživatelích k zobrazování reklam, včetně personalizované nebo zájmově orientované reklamy,
  - přenos, prodej nebo používání údajů o uživatelích ke zjištění úvěruschopnosti nebo k poskytování úvěrů,
  - přenos, prodej nebo používání údajů o uživatelích s jakýmkoli produktem nebo službou, které lze kvalifikovat jako lékařské zařízení podle paragrafu 201(h) federálního zákona o potravinách, léčivech a kosmetických prostředcích (Federal Food, Drug and Cosmetic Act), pokud budou údaje o uživatelích lékařským zařízením použity k plnění jeho regulované funkce,
  - přenos, prodej nebo používání údajů o uživatelích k jakémukoliv účelu nebo jakýmkoliv způsobem, který se týká chráněných zdravotních údajů (podle definice v zákoně HIPAA), pokud k takovému použití nedostanete od společnosti Google předchozí písemný souhlas.

Minimální rozsah

Smíte žádat jen o taková oprávnění, která jsou nezbytná k implementaci funkcí nebo služeb vašeho produktu. Žádosti o přístup musí být konkrétní a omezená jen na nezbytná data.

Transparentní a přesné oznámení a kontrola

Health Connect spravuje údaje o zdraví a kondici, včetně citlivých údajů, a vyžaduje, aby všechny aplikace měly komplexní zásady ochrany soukromí. V zásadách ochrany soukromí musí být transparentně zveřejněno, jak aplikace shromažďuje, používá a sdílí údaje o uživatelích. Kromě splnění zákonných požadavků musí vývojáři v zásadách ochrany soukromí zveřejnit následující informace:

- Přesný popis aplikace a toho, k jakým datům přistupuje a jak tato data souvisejí s jejími hlavními funkcemi nebo doporučeními.
- Postupy v oblasti uchovávání a mazání dat.
- Postupy nakládání s daty. K přenosu dat je například nutné používat moderní kryptografii (například pomocí protokolu HTTPS).

Bezpečná manipulace s daty

Veškeré údaje o uživatelích musíte zpracovávat zabezpečeným způsobem. Přijměte přiměřená a vhodná opatření k ochraně všech aplikací nebo systémů, které využívají službu Health Connect, před neoprávněným nebo nezákonným přístupem, použitím, zničením, ztrátou, změnou nebo zveřejněním.

Mezi doporučené bezpečnostní postupy patří zavedení a udržování systému řízení bezpečnosti informací, jak je uvedeno v normě ISO/IEC 27001, a zajištění, aby aplikace nebo webová služba byla robustní a bez běžných bezpečnostních problémů, jak je uvedeno v seznamu OWASP Top 10.

Pokud váš produkt přenáší data mimo vlastní zařízení uživatele, v závislosti na rozhraní API, ke kterému přistupujete, a počtu oprávnění udělených uživateli nebo počtu uživatelů budeme vyžadovat, aby vaše

aplikace nebo služba prošla pravidelným hodnocením zabezpečení a získala písemné posouzení od určené třetí strany.

Další informace o požadavcích na aplikace, které se připojují ke službě Health Connect, naleznete v tomto článku nápovědy.

Služba VPN

VpnService je základní třída pro aplikace, které rozšiřují a vytvářejí vlastní řešení VPN. Pouze aplikace, které používají třídu VpnService a ;mají VPN jako svou základní funkci, mohou vytvořit bezpečný tunel na úrovni zařízení ke vzdálenému serveru. Výjimkou jsou aplikace, které vyžadují vzdálený server pro základní funkce, jako jsou:

- aplikace pro rodičovskou kontrolu a podnikovou správu,
- sledování využití aplikace,
- aplikace k zabezpečení zařízení (například antivir, správa mobilních zařízení, firewall),
- nástroje související se sítí (například vzdálený přístup),
- aplikace k procházení webu,
- aplikace operátora, které vyžadují funkce VPN k poskytování služeb telefonu nebo připojení.

Třídu VpnService není dovoleno používat k následujícím účelům:

- shromažďování osobních a citlivých údajů o uživatelích bez oznámení na viditelném místě a souhlasu,
- přesměrování nebo úprava provozu uživatelů z jiných aplikací na zařízení za účelem zpeněžení (například přesměrování reklamního provozu přes jinou zemi, než je země uživatele),

Aplikace, které používají třídu VpnService, musí:

- zdokumentovat použití třídy VpnService v záznamu na Google Play,
- šifrovat data přenášená ze zařízení do koncového bodu tunelu VPN,
- dodržovat všechny programové zásady pro vývojáře , včetně zásad týkajících se reklamních podvodů , oprávnění a malwaru .

Oprávnění pro přístup k přesným budíkům

Počínaje Androidem 13 (cílová úroveň API 33) bude zavedeno nové oprávnění USE_EXACT_ALARM, které aplikacím bude umožňovat přístup k funkci přesných budíků .

USE_EXACT_ALARM je omezené oprávnění a aplikace toto oprávnění smějí deklarovat pouze v případě, že jejich základní funkce vyžaduje přístup k přesným budíkům. Aplikace požadující toto omezené oprávnění podléhají kontrole. Pokud nebudou splňovat kritéria přijatelného použití, nebude je možné na Google Play publikovat.

Přijatelné případy použití oprávnění pro přístup k přesným budíkům

Funkci USE_EXACT_ALARM smí aplikace používat pouze v případě, že její základní funkce pro uživatele vyžaduje přesně načasované akce. Příklady:

- Aplikace je budík nebo časovač.
- Jedná se o kalendářovou aplikaci, která zobrazuje upozornění na události.

Pokud funkci přesných budíků používáte k něčemu, co není popsáno výše, měli byste zvážit, zda by jako alternativu nebylo možné použít oprávnění SCHEDULE_EXACT_ALARM.

Další informace o funkci přesných budíků naleznete v těchto pokynech pro vývojáře .

Oprávnění k zobrazení objektu intent na celou obrazovku

U aplikací, které cílí na Android 14 (cílová úroveň rozhraní API 34) a vyšší, je oprávnění USE_FULL_SCREEN_INTENT považováno za oprávnění aplikací ke speciálnímu přístupu .

Oprávnění USE_FULL_SCREEN_INTENT bude aplikaci automaticky uděleno pouze v případě, že její hlavní funkce spadají do jedné z níže uvedených kategorií, které vyžadují upozornění s vysokou prioritou:

- nastavení budíku,
- přijímání telefonních hovorů nebo videohovorů.

Aplikace, které žádají o toto oprávnění, podléhají kontrole, a pokud nesplňují výše uvedená kritéria, toto oprávnění jim nebude automaticky uděleno. V takovém případě musí aplikace o povolení k použití oprávnění USE_FULL_SCREEN_INTENT požádat uživatele.

Připomínáme, že jakékoli použití oprávnění USE_FULL_SCREEN_INTENT musí být v souladu se všemi zásadami služby Google Play pro vývojáře, včetně zásad ohledně nežádoucího softwaru pro mobilní zařízení, zneužívání zařízení a sítí a reklam. Oznámení prostřednictvím intentů na celou obrazovku nesmějí narušovat fungování zařízení uživatele, poškozovat ho ani k němu přistupovat neoprávněným způsobem. Aplikace také nesmí zasahovat do jiných aplikací ani narušovat použitelnost zařízení.

Další informace o oprávnění USE_FULL_SCREEN_INTENT naleznete v našem centru 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 sítě autorizovaného operátora), popř. které je narušují, poškozují nebo v nich získávají neoprávněný přístup.

Aplikace na Google Play musejí splnit požadavky na optimalizaci pro výchozí systém Android popsané v pokynech pro zajištění kvality aplikací na Google Play .

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

Aplikace nebo kód třetí strany (např. sady SDK) v interpretovaných jazycích (JavaScript, Python, Lua atd.) načítané za běhu (tj. kód není součástí balíčku aplikace) nesmějí umožňovat potenciální porušení zásad Google Play.

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:

Příklady běžných porušení zásad ohledně zneužívání zařízení a sítí:

- 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 třetích stran (například 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.
- Aplikace nebo kód třetí strany (např. sady SDK) obsahující zobrazení WebView s rozhraními JavaScriptu, která načítají nedůvěryhodný webový obsah (např. adresy URL se schématem http://) nebo neověřené adresy URL získané z nedůvěryhodných zdrojů (např. z nedůvěryhodných intentů).
- Aplikace, které používají oprávnění pro intenty na celou obrazovku k vynucení uživatelské interakce s rušivými reklamami nebo oznámeními.

Použití služby v popředí

Oprávnění Služba v popředí zajišťuje správné používání služeb v popředí pro uživatele. U aplikací, které cílí na Android 14 a vyšší, musíte pro každou službu v popředí použitou v aplikaci zadat platný typ služby v popředí a deklarovat oprávnění služby v popředí, které je pro daný typ vhodné. Pokud například v aplikaci potřebujete geolokaci v mapě, musíte v manifestu aplikace deklarovat oprávnění FOREGROUND_SERVICE_LOCATION .

Oprávnění služby v popředí mohou aplikace deklarovat pouze v případě, že použití:

- poskytuje funkci, která je užitečná pro uživatele a je relevantní k hlavní funkci aplikace,
- je iniciováno uživatelem nebo ho uživatel může zaznamenat (např. zvuk z přehrávání skladby, odesílání médií do jiného zařízení, přesné a jasné oznámení uživateli, žádost uživatele o nahrání fotky do cloudu),
- může uživatel ukončit nebo zastavit,
- nemůže být systémem přerušeno nebo odloženo, aniž by to mělo negativní dopad na uživatelský dojem nebo způsobilo, že uživatelem očekávaná funkce nebude fungovat tak, jak má (např. telefonní hovor musí začít okamžitě a systém ho nemůže odložit),
- běží pouze tak dlouho, jak je nutné k dokončení úkolu.

Výše uvedená kritéria se nevztahují na následující případy použití služeb v popředí:

- typy služeb v popředí systemExempted a shortService ,
- typ služby v popředí dataSync pouze při použití funkcí Play Asset Delivery .

Použití služby v popředí je dále vysvětleno zde.

Úlohy přenosu dat iniciované uživateli

API pro uživatelem spouštěné úlohy přenosu dat mohou aplikace používat pouze v případě, že použití:

- iniciuje uživatel,
- slouží pro úlohy síťového přenosu dat,
- běží pouze po dobu nezbytně nutnou k dokončení přenosu dat.

Použití rozhraní API pro přenos dat iniciovaný uživatelem je dále vysvětleno zde.

Požadavky na označení Flag Secure

FLAG_SECURE je příznak zobrazení deklarovaný v kódu aplikace, který značí, že její uživatelské rozhraní obsahuje citlivá data, která mají být při používání aplikace omezena na zabezpečené platformy. Tento příznak je navržen tak, aby zabránil zobrazení dat ve snímcích obrazovek nebo zobrazení na nezabezpečených displejích. Vývojáři tento příznak deklarují v případě, že obsah aplikace nemá být vysílán, prohlížen nebo jinak přenášen mimo aplikaci nebo zařízení uživatelů.

Kvůli zabezpečení a ochraně soukromí musí všechny aplikace distribuované na Google Play respektovat deklaraci FLAG_SECURE ostatních aplikací. To znamená, že aplikace nesmějí zprostředkovávat ani vytvářet řešení k obcházení nastavení FLAG_SECURE v jiných aplikacích.

Aplikace kvalifikované jako nástroje pro usnadnění přístupu jsou z tohoto požadavku vyjmuty. Nesmějí však obsah chráněný příznakem FLAG_SECURE přenášet ani ukládat (ani do mezipaměti) pro přístup mimo zařízení uživatele.

Aplikace, ve kterých běží kontejnery Android v zařízení

Kontejnerové aplikace pro Android na zařízení poskytují prostředí, která simulují celý základní operační systém Android nebo jeho části. Tato prostředí nemusí zahrnovat kompletní sadu zabezpečovacích funkcí systému Android . Vývojáři proto do manifestu mohou přidat příznak zabezpečeného prostředí, který kontejnerům Android na zařízeních sděluje, že aplikaci není dovoleno spouštět v jejich simulovaném prostředí Android.

Příznak manifestu bezpečného prostředí

REQUIRE_SECURE_ENV je příznak, jehož deklarováním lze v manifestu aplikace uvést, že ji není dovoleno spouštět v kontejnerových aplikacích Android na zařízeních. Aplikace, které na zařízeních poskytují kontejnery Android, musejí z důvodu zajištění bezpečnosti a ochrany soukromí deklaraci tohoto příznaku respektovat a také musí splňovat tyto požadavky:

- U aplikací, které se pokoušejí načíst do svého kontejneru Android v zařízení, musejí kontrolovat, zda jejich manifest neobsahuje tento příznak.
- Nesmějí do svého kontejneru Android v zařízení načítat aplikace, které deklarovaly tento příznak.
- Nesmějí fungovat jako prostředníci a zachytáváním či voláním rozhraní API vyvolávat dojem, že jsou nainstalována v kontejneru.
- Nesmějí umožňovat obejití tohoto příznaku (např. načítat starší verzi aplikace s cílem obejít příznak REQUIRE_SECURE_ENV aktuální aplikace).

Více informací o těchto zásadách najdete v našem centru nápovědy.

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/videa 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.

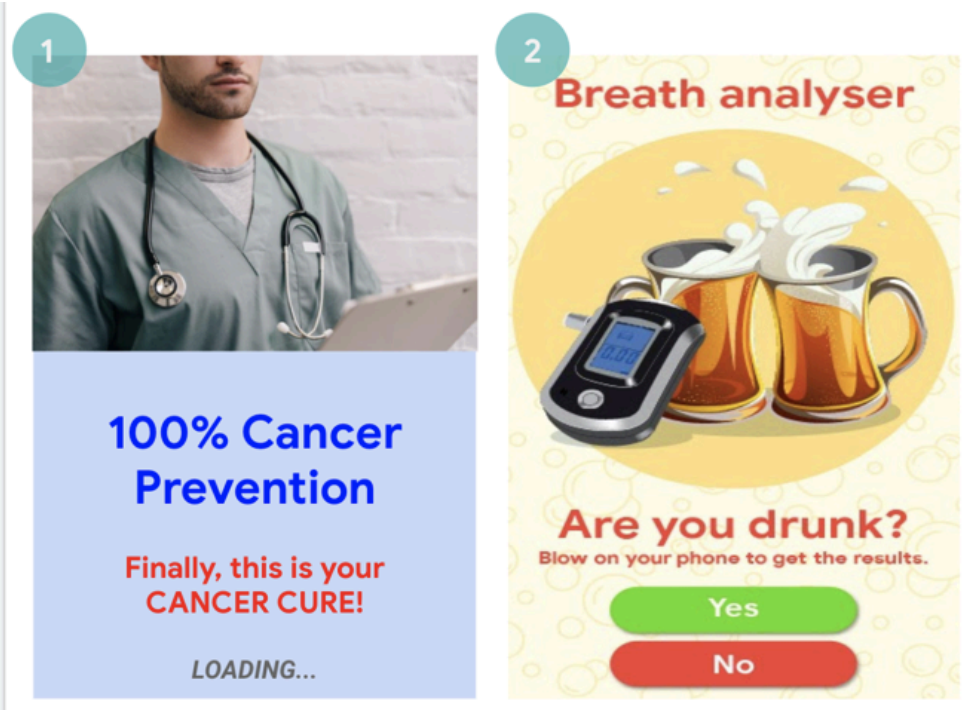
Zavádějící tvrzení

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.
- 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).
- Zjevně klamavý nebo falešný obsah, který může ovlivnit volby nebo který nepravdivě informuje o výsledcích voleb.

- Aplikace, které falešně uvádějí spojení s veřejnoprávním subjektem nebo zprostředkování státních služeb, 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, které obsahují zavádějící lékařské údaje nebo údaje týkající se zdraví (léčba rakoviny).
(2) Aplikace, které tvrdí, že obsahuje funkce, které nelze implementovat (použití telefonu jako dechového analyzátoru).

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, bankovních účtů 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 uživatelích, 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 sítí CDN, aniž by uživatele před zahájením stahování informovaly o velikosti stahovaného obsahu a požádaly o svolení.

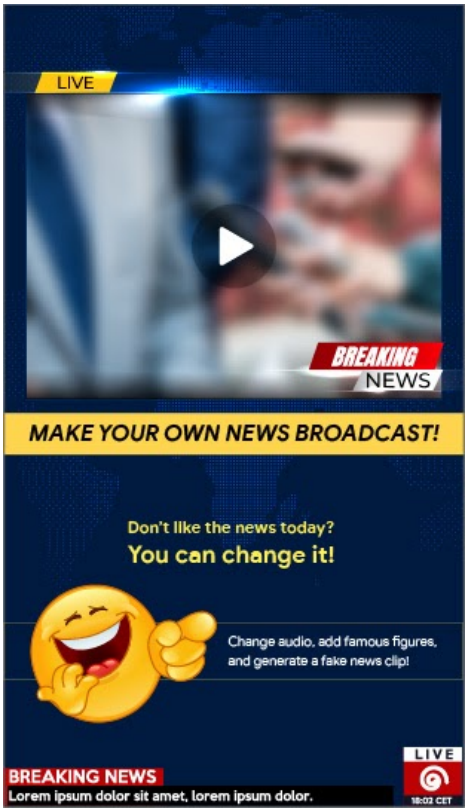
Manipulace s médii

Nepovolujeme aplikace, které pomocí snímků, zvuku, 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.

Transparentnost chování

Funkce aplikace musí být pro uživatele jasně srozumitelná. Nezahrnujte skryté a nezdokumentované funkce ani funkce čekající na aktivaci. Není dovoleno vyhýbat se recenzím. U aplikací může být vyžadováno poskytnutí dalších podrobností k zajištění bezpečnosti uživatelů, integrity systému a dodržování zásad.

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.

Zásady o cílové úrovni rozhraní API na Google Play

Aby bylo zajištěno bezpečné prostředí pro uživatele, Google Play pro **všechny aplikace** vyžaduje následující cílové úrovně rozhraní API:

Nové aplikace a aktualizace aplikací MUSÍ cílit na úroveň rozhraní API Android starou max. jeden rok od posledního vydání velké verze Androidu. Nové aplikace a aktualizace aplikací, které tento požadavek nesplní, nebude možné přes Play Console odesílat.

Existující aplikace na Google Play, které nejsou aktualizované a které necílí na úroveň rozhraní API Android starou max. dva roky od posledního vydání velké verze Androidu, nebudou k dispozici pro nové uživatele s novějšími verzemi systému Android.Uživatelé, kteří si danou aplikaci dříve nainstalovali z Google Play, ji budou moci zobrazit, opětovně nainstalovat a používat na jakékoli verzi Androidu, kterou aplikace podporuje.

Technické rady ohledně toho, jak splnit požadavek na cílovou úroveň rozhraní API, najdete v průvodci migrací .

Přesnou časovou osu a výjimky najdete v tomto článku centra nápovědy .

Požadavky na sady SDK

K integraci klíčových funkcí a služeb do svých aplikací vývojáři často používají kód třetích stran (například sady SDK). Když do své aplikace zahrnete sadu SDK, měli byste se ujistit, že své uživatele a aplikaci dokážete ochránit před všemi chybami zabezpečení. V této části ukazujeme, jak se některé z našich stávajících požadavků na ochranu soukromí a zabezpečení uplatňují v kontextu sad SDK a jak vývojářům pomáhají s bezpečnou integrací sad SDK do aplikací.

Pokud do své aplikace zahrnete sadu SDK, nesete odpovědnost za to, že kód a postupy třetích stran nezpůsobí porušení programových zásad služby Google Play pro vývojáře. Je důležité vědět, jak sady SDK použité v aplikaci zacházejí s údaji o uživatelích, která oprávnění používají a jaká data a proč shromažďují. Mějte na paměti, že shromažďování a zpracování údajů o uživatelích pomocí sady SDK musí odpovídat používání těchto dat ve vaší aplikaci v souladu se zásadami.

Důkladně se seznamte se všemi níže uvedenými zásadami a existujícími požadavky zásad, které se týkají sad SDK, a zajistěte, abyste je neporušovali.

Zásady pro údaje o uživatelích

Musíte být transparentní ohledně toho, jak zacházíte s údaji o uživatelích (například s informacemi, které jste o nich a jeho zařízeních shromáždili). To znamená, že musíte zveřejňovat informace o přístupu, shromažďování, využívání, sdílení údajů o uživatelích z vaší aplikace a nakládání s nimi a také musíte omezit využití údajů na účely, které jsou v souladu se zásadami a o nichž uživatele informujete.

Pokud do aplikace zahrnete kód třetí strany (například sady SDK), musíte zajistit, aby tento kód a postupy této třetí strany ve vztahu k údajům o uživatelích z vaší aplikace neporušovaly programové zásady pro vývojáře Google Play, které zahrnují požadavky na používání a zveřejněné informace. Musíte například zajistit, aby vaši poskytovatelé sad SDK neprodávali osobní a citlivé údaje o uživatelích z vaší aplikace. Tento požadavek platí bez ohledu na to, zda jsou údaje o uživatelích přenášeny po odeslání na server nebo prostřednictvím vložení kódu třetí strany do vaší aplikace.

Osobní a citlivé údaje o uživatelích

- Shromažďování, využívání a sdílení osobních a citlivých údajů získaných prostřednictvím aplikace musíte omezit pouze na funkce aplikace a služeb a pouze na účely, které jsou v souladu se zásadami a přiměřeným očekáváním uživatelů:
  - Aplikace, které využívají osobní a citlivé údaje o uživatelích k zobrazování reklam, musí splňovat zásady inzerce služby Google Play.
- Všechny osobní a citlivé údaje o uživatelích musíte zpracovávat zabezpečeným způsobem včetně přenosu šifrovaného moderními metodami (např. pomocí protokolu HTTPS).
- Pokud je to možné, před přístupem k údajům pomocí oprávnění systému Android používejte žádost o oprávnění za běhu.

Prodej osobních a citlivých údajů o uživatelích

Osobní a citlivé údaje o uživatelích nesmíte prodávat.

- „Prodej“ znamená výměnu nebo přenos osobních a citlivých údajů o uživatelích třetí straně za peněžní úplatu.

- Za prodej není považován přenos osobních a citlivých údajů iniciovaný uživatelem (například když uživatel pomocí funkce aplikace přenáší soubor třetí straně nebo když se rozhodne použít speciální aplikaci pro výzkumnou studii).

Požadavky na viditelné oznámení a souhlas

V případě, kdy vaše aplikace využívá přístup k osobním a citlivým údajům uživatelů, shromažďuje je, používá nebo sdílí a kdy tyto aktivity nemusejí být v souladu s rozumným očekáváním uživatelů příslušné služby nebo funkce, musíte splnit požadavky na viditelné oznámení a souhlas uvedené v zásadách pro údaje o uživatelích.

Pokud aplikace obsahuje kód třetí strany (například sady SDK), který je určen k automatickému shromažďování osobních a citlivých údajů o uživatelích, musíte do dvou týdnů od přijetí žádosti od Google Play (nebo v rámci delšího časového období uvedeného v žádosti služby Google Play) poskytnout dostatečný důkaz prokazující, že aplikace splňuje požadavky těchto zásad na viditelné oznámení a souhlas, včetně požadavků na čtení, shromažďování, používání a sdílení údajů prostřednictvím kódu třetí strany.

Zajistěte, aby použití kódu třetí strany (například sady SDK) v aplikaci nevedlo k porušení zásad pro údaje o uživatelích.

Další informace o požadavcích na oznámení na viditelném místě a souhlas najdete v tomto článku centra nápovědy.

Příklady porušení zásad způsobených sadami SDK

- aplikace se sadou SDK, která shromažďuje osobní a citlivé údaje o uživatelích a nezachází s těmito údaji jako s údaji podléhajícími těmto zásadám pro údaje o uživatelích, včetně přístupu k údajům, nakládání s údaji (včetně nepovoleného prodeje) a požadavků na viditelné oznámení a souhlas,
- aplikace se sadou SDK, která ve výchozím nastavení shromažďuje osobní a citlivé údaje o uživatelích v rozporu s požadavky těchto zásad na souhlas uživatele a zveřejnění na viditelném místě,
- aplikace se sadou SDK, která uvádí, že osobní a citlivé údaje o uživatelích shromažďuje pouze k poskytování ochrany před podvody a zneužitím, ale ve skutečnosti shromážděná data také sdílí se třetími stranami pro účely inzerce nebo analýzy,
- aplikace se sadou SDK, která odesílá informace o nainstalovaných balíčcích uživatelů a nesplňuje při tom požadavky na oznámení na viditelném místě a/nebo zásady.
  - Přečtěte si také zásady ohledně nevyžádaného softwaru pro mobilní zařízení.

Další požadavky na přístup k osobním a citlivým údajům

Požadavky pro jednotlivé činnosti jsou popsány v tabulce níže.

Aktivita	Požadavek
Aplikace shromažďuje nebo odkazuje na trvalé identifikátory zařízení (např. IMEI, IMSI, sériové číslo SIM karty apod.)	Trvalé identifikátory zařízení nesmí být propojeny s jinými osobními a citlivými údaji o uživatelích ani resetovatelnými identifikátory zařízení pro účely: • telefonických služeb spojených s identitou SIM karty (např. volání přes Wi-Fi spojené s účtem u operátora), • podnikových aplikací pro správu zařízení, které využívají režim vlastníka zařízení. Tyto způsoby využití musí být uživatelům viditelně oznámeny, jak je uvedeno v zásadách pro údaje o uživatelích . Alternativní unikátní identifikátory jsou popsány zde . Další pokyny v souvislosti s inzertním ID Android naleznete v zásadách inzerce .
Aplikace cílí na děti	Aplikace může obsahovat pouze sady SDK, které mají vlastní certifikaci k použití ve službách určených pro děti. Úplné znění zásad a požadavky naleznete v části Program sad SDK pro reklamy s vlastní certifikací pro rodiny.

Příklady porušení zásad způsobených sadami SDK

- aplikace využívající sadu SDK, která spojuje Android ID s polohou,

- aplikace se sadou SDK, která spojuje AAID s trvalými identifikátory zařízení pro jakékoli reklamní nebo analytické účely,
- aplikace využívající sadu SDK, která spojuje AAID s e-mailovou adresou pro účely analýzy.

Sekce Zabezpečení údajů

Každý vývojář musí u každé své aplikace vyplnit sekci Zabezpečení údajů, ve které popíše shromažďování, využití a předávání údajů o uživatelích. Týká se to i dat shromážděných a zpracovávaných prostřednictvím knihoven nebo sad SDK třetích stran, které vývojáři ve svých aplikacích používají. Vývojář ručí za přesnost a aktuálnost štítku a uvedených informací. Pokud je to relevantní, údaje v sekci musí být v souladu s oznámeními v zásadách ochrany soukromí aplikace.

Další informace o vyplnění sekce Zabezpečení údajů naleznete v tomto článku centra nápovědy.

Přečtěte si úplné zásady pro údaje o uživatelích.

Zásady pro oprávnění a rozhraní API s přístupem k citlivým údajům

Žádosti o oprávnění a rozhraní API, která mají přístup k citlivým údajům, musí uživatelům dávat smysl. Můžete žádat pouze o oprávnění a rozhraní API s přístupem k citlivým údajům, která jsou nezbytná k implementaci existujících funkcí nebo služeb v aplikaci, které propagujete v záznamu na Google Play. Nesmíte používat oprávnění nebo rozhraní API s přístupem k citlivým údajům, která umožňují přístup k údajům o uživateli nebo zařízení za účelem využití v neuvedených, neimplementovaných nebo nedovolených funkcích. Osobní a citlivé údaje získané prostřednictvím oprávnění nebo rozhraní API s přístupem k citlivým údajům je zakázáno prodávat nebo sdílet za účelem zprostředkování prodeje.

Viz úplné zásady pro oprávnění a rozhraní API s přístupem k citlivým údajům.

Příklady porušení zásad způsobených sadami SDK

- Aplikace obsahuje sadu SDK, která na pozadí žádá o informace o poloze k nepovoleným nebo nezveřejněným účelům.
- Aplikace obsahuje sadu SDK, která bez souhlasu uživatele přenáší číslo IMEI získané pomocí oprávnění read_phone_state systému Android.

Zásady ohledně malwaru

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

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

Požadavky těchto zásad se vztahují také na jakýkoli kód třetí strany (například na sady SDK), který do své aplikace zahrnete.

Pročitajte cjelovita pravila o zlonamjernom softveru.

Primjeri kršenja koje je uzrokovao SDK

- aplikace, která obsahuje knihovny SDK od poskytovatelů, kteří distribuují škodlivý software,
- aplikace, která porušuje model oprávnění systému Android či krade identifikační údaje (například tokeny OAuth) jiných aplikací,
- aplikace, která zneužívá některé funkce k tomu, aby ji nebylo možné odinstalovat či vypnout,
- aplikace, která deaktivuje SELinux,

- aplikace zahrnující sadu SDK, která porušuje model oprávnění systému Android tím, že získává zvýšená oprávnění prostřednictvím přístupu k datům v zařízení k neuvedenému účelu,
- aplikace zahrnující sadu SDK s kódem, který se uživatele klamavě pokouší přimět k předplacení obsahu přes fakturu za mobilní telefonní služby.

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

Spyware

Spyware je škodlivá aplikace, kód nebo chování, které shromažďuje, exfiltruje nebo předává data uživatelů nebo data ze zařízení, aniž by to souviselo s funkcemi, které jsou v souladu se zásadami.

Škodlivý kód nebo chování, které lze považovat za špehování uživatele nebo exfiltraci dat bez odpovídajícího oznámení nebo souhlasu, jsou také považovány za spyware.

Viz úplné zásady ohledně spywaru.

Příklady porušení zásad ohledně spywaru způsobených sadami SDK:

- Aplikace, která používá sadu SDK přenášející data ze zvukových nahrávek nebo nahrávek hovorů, i když to nesouvisí s funkcí aplikace v souladu se zásadami.
- Aplikace se škodlivým kódem třetí strany (například sadou SDK), která přenáší data ze zařízení způsobem, který je pro uživatele neočekávaný a/nebo bez odpovídajícího oznámení uživateli nebo souhlasu od uživatele.

Zásady ohledně nevyžádaného softwaru pro mobilní zařízení

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.

Příklady porušení zásad:

- inzertní podvody,
- sociální inženýrství.

Ochrana údajů o uživatelích

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

Příklady porušení zásad:

- shromažďování dat (srov. Spyware),
- zneužití omezených oprávnění.

Viz úplné zásady ohledně nevyžádaného softwaru pro mobilní zařízení

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

Aplikace nebo kód třetí strany (např. sady SDK) v interpretovaných jazycích (JavaScript, Python, Lua atd.) načítané za běhu (tj. kód není součástí balíčku aplikace) nesmějí umožňovat potenciální porušení zásad Google Play.

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.

Přečtěte si úplné zásady ohledně zneužívání zařízení a sítí.

Příklady porušení zásad způsobených sadami SDK

- 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.
- Vaše aplikace zahrnuje sadu SDK, která stahuje spustitelný kód, jako jsou soubory dex nebo nativní kód, z jiného zdroje než z Google Play.
- Vaše aplikace zahrnuje sadu SDK se zobrazeními WebView s rozhraními JavaScriptu, která načítají nedůvěryhodný webový obsah (např. adresy URL se schématem http://) nebo neověřené adresy URL získané z nedůvěryhodných zdrojů (např. z nedůvěryhodných objektů Intent).
- Vaše aplikace zahrnuje sadu SDK, která obsahuje kód k aktualizaci svého vlastního souboru APK.
- Vaše aplikace zahrnuje sadu SDK, která uživatele vystavuje ohrožení zabezpečení stahováním souborů přes nezabezpečené připojení.
- Vaše aplikace používá sadu SDK, která obsahuje kód ke stažení nebo instalaci aplikací z neznámých zdrojů mimo Google Play.
- Vaše aplikace zahrnuje sadu SDK, která používá služby v popředí k nepovoleným účelům.
- Vaše aplikace zahrnuje sadu SDK, která používá služby v popředí k účelům, které zásady povolují, ale v manifestu aplikace to není deklarováno.

Zásady týkající se klamavého 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/videa 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.

Přečtěte si úplné zásady ohledně klamavého chování.

Transparentnost chování

Funkce aplikace musí být pro uživatele jasně srozumitelná. Nezahrnujte skryté a nezdokumentované funkce ani funkce čekající na aktivaci. Není dovoleno vyhýbat se recenzím. U aplikací může být vyžadováno poskytnutí dalších podrobností k zajištění bezpečnosti uživatelů, integrity systému a dodržování zásad.

Příklad porušení zásad, které způsobila sada SDK

- Aplikace obsahuje sadu SDK, která slouží k vyhýbání se recenzím.

Které zásady pro vývojáře Google Play jsou v důsledku použití sad SDK nejčastěji porušovány?

Prostudujte si všechny následující zásady. Pomůže vám to zajistit, aby kód třetích stran použitý ve vaší aplikaci splňoval zásady služby Google Play pro vývojáře:

- Zásady pro údaje o uživatelích
- Oprávnění a rozhraní API s přístupem k citlivým údajům
- Zásady ohledně zneužívání zařízení a sítí
- malware,
- nevyžádaný software pro mobilní zařízení
- Program sad SDK pro reklamy s vlastní certifikací pro rodiny
- Zásady inzerce
- Klamavé chování

- Programové zásady služby Google Play pro vývojáře

K porušení těchto zásad dochází nejčastěji. Špatný kód sad SDK však u aplikace může vést i k porušení jiných zásad, které výše nejsou uvedeny. Nezapomeňte si prostudovat všechny zásady a sledovat jejich aktuální znění, protože jako vývojář aplikací odpovídáte za to, aby sady SDK ve vaší aplikaci nakládaly s jejími daty v souladu se zásadami.

Další informace najdete v centru nápovědy.

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). Na základě tohoto základního principu se snažíme poskytovat uživatelům a jejich zařízením Android bezpečný ekosystém. Malware je každý kód, který by mohl uživatele, jejich data či zařízení vystavit riziku. Mezi malware patří například potenciálně škodlivé aplikace, binární kódy a úpravy aplikačních rámců a dělí se do různých kategorií, jako jsou trojské koně, phishing a spyware, přičemž kategorie neustále aktualizujeme a přidáváme nové.

Požadavky těchto zásad se vztahují také na jakýkoli kód třetí strany (například na sady SDK), který do své aplikace zahrnete.

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 starou verzi 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 služba Google Play Protect může klasifikovat jako chybu zabezpečení.

Fakturační podvod

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

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

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

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

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

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

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

Stalkerware

Kód, který ze zařízení shromažďuje osobní nebo citlivé údaje o uživatelích a přenáší data třetí straně (podniku nebo jiné osobě) pro účely sledování.

Aplikace musí poskytnout náležité oznámení na viditelném místě a získat souhlas, jak to vyžadují zásady pro údaje o uživatelích .

Pokyny ohledně sledovacích aplikací

Jedinými přijatelnými sledovacími aplikacemi jsou aplikace navržené a distribuované výhradně za účelem sledování jiné osoby (například sledování dětí v rámci rodičovské kontroly nebo sledování jednotlivých zaměstnanců v rámci firemní správy), které jsou plně v souladu s níže uvedenými požadavky. Pomocí těchto aplikací není dovoleno sledovat jinou osobu (například manžela nebo manželku) bez jejího vědomí a svolení, a to ani v případě, že aplikace zobrazuje trvalé oznámení. Tyto aplikace musí být označeny jako sledovací pomocí značky metadat IsMonitoringTool v souboru manifestu.

Sledovací aplikace musí splňovat tyto požadavky:

- Nesmějí se prezentovat jako řešení určené ke špehování nebo skrytému sledování.
- Nesmějí skrývat ani maskovat sledovací funkce ani o nich uživatelům poskytovat zavádějící informace.
- Musejí uživatelům po celou dobu běhu zobrazovat trvalé oznámení a jedinečnou ikonu, která aplikaci jasně identifikuje.
- Funkce sledování musí být uvedena v popisu aplikace v obchodu Google Play.
- Aplikace a záznamy aplikací na Google Play nesmějí žádným způsobem umožňovat aktivaci nebo použití funkcí, které porušují tyto podmínky (například prostřednictvím odkazů na soubory APK hostované mimo Google Play, které nesplňují tyto zásady).

- Aplikace musí splňovat všechny platné předpisy. Za to, zda vaše aplikace v cílovém národním prostředí neporušuje zákony, nesete výhradní zodpovědnost vy.

Další informace najdete v článku centra nápovědy Použití příznaku isMonitoringTool .

Odepření služby (DoS)

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

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

Nepřátelské stahovací programy

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

O nepřátelské stahování se může jednat za těchto podmínek:

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

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

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

Hrozba pro jiné systémy než Android

Kód, který obsahuje hrozby pro jiné systémy než Android.

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

Phishing

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

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

Zneužití zvýšených oprávnění

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

Příklady:

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

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

Ransomware

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

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

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

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

Rootování

Kód, který rootuje zařízení.

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

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

Spam

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

Spyware

Spyware je škodlivá aplikace, kód nebo chování, které shromažďuje, exfiltruje nebo předává data uživatelů nebo data ze zařízení, aniž by to souviselo s funkcemi, které jsou v souladu se zásadami.

Škodlivý kód nebo chování, které lze považovat za špehování uživatele nebo exfiltraci dat bez odpovídajícího oznámení nebo souhlasu, jsou také považovány za spyware.

Za porušení zásad ohledně spywaru jsou považovány mimo jiné tyto činnosti:

- Nahrávání zvuku nebo hovorů na telefonu
- Krádež dat aplikací
- Aplikace se škodlivým kódem třetí strany (například sadou SDK), která přenáší data ze zařízení způsobem, který je pro uživatele neočekávaný a/nebo bez odpovídajícího oznámení uživateli nebo souhlasu od uživatele.

Všechny aplikace musí také splňovat všechny programové zásady služby Google Play pro vývojáře, včetně zásad týkajících se uživatelských dat a dat ze zařízení, jako jsou zásady Nevyžádaný software pro mobilní zařízení, Uživatelská data, Oprávnění a rozhraní API s přístupem k citlivým údajům a Požadavky na sady SDK.

Trojský kůň

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

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

Poznámka ohledně neobvyklých aplikací

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

Poznámka ke kategorii Zpětná vrátka

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

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

Maskware

Aplikace, která používá vyhýbavé praktiky, aby uživateli poskytla odlišné nebo falešné funkce. Tyhle aplikace se maskují jako legitimní aplikace nebo hry, aby pro obchody s aplikacemi působily neškodně, a skrývají škodlivý obsah pomocí obfuskace, dynamického načítání kódu a podobných praktik.

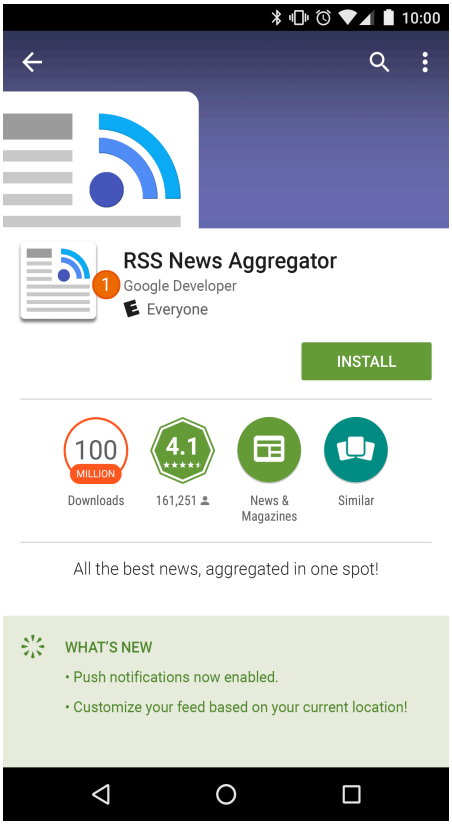
Maskware se podobná ostatním kategoriím potenciálně škodlivých aplikací (zejména trojským koňům), hlavní rozdíl spočívá ve způsobu maskování škodlivé aktivity.

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.

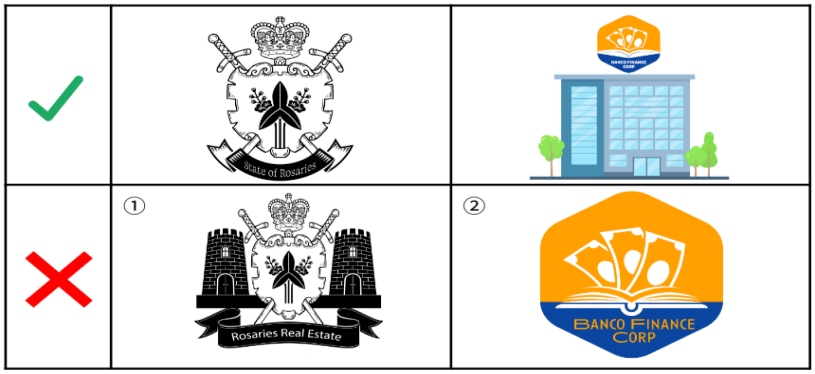
Příklady běžných porušení zásad:

- Vývojáři, kteří nepravdivě naznačují vztah k jiné společnosti/vývojáři/subjektu/organizaci:



① Jméno vývojáře uvedené u této aplikace naznačuje oficiální vztah ke společnosti Google, přestože žádný takový vztah neexistuje.

- Aplikace, jejichž ikony a názvy nepravdivě naznačují vztah s jinou společností/vývojářem/subjektem/organizací.



①Aplikace používá státní znak a klame uživatele, aby se domnívali, že je spojena se státními úřady.
②Aplikace kopíruje logo obchodního subjektu a nepravdivě tím naznačuje, že se jedná o oficiální aplikaci dané firmy.

- Názvy a ikony aplikace jsou natolik podobné názvům nebo ikonám existujících produktů či služeb, že to může být pro uživatele zavádějící.

①V ikoně aplikace je použito logo oblíbené webové stránky s kryptoměnami, čímž aplikace naznačuje, že se jedná o oficiální web.
②V ikoně aplikace jsou použity postava a název slavného televizního pořadu, čímž aplikace uživatelům klamavě naznačuje, že je spojena s televizním pořadem.

- Aplikace, které nepravdivě uvádějí, že jsou oficiální aplikací zavedeného subjektu. Bez potřebných oprávnění nebo práv nelze používat například názvy jako Oficiální aplikace Karla Gotta.
- Aplikace porušující pokyny pro použití značky Android .

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 softwaruuvedeno, 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 vysvětlete, 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 zavirován).
- 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,
- sociální inženýrství.

Ochrana soukromí a dat uživatelů

Jasně a transparentně vysvětlete způsob používání, shromažďování a sdílení osobních a citlivých údajů o uživatelích a přístup k nim. Použití údajů o uživatelích musí být pokud možno v souladu se všemi příslušnými zásadami ohledně údajů o uživatelích 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 uživatelích, které shromáždíte, 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 uživatelích na servery přenášet pouze v případě, že je tento přenos spojen s funkčností aplikace.
- Nevyžadujte po uživatelích, aby vypnuli bezpečnostní ochrany zařízení, jako je služba Google Play Protect, a nesnažte se je k tomu ani přimět. Uživatelům například nesmíte nabízet další funkce aplikace ani odměny výměnou za vypnutí služby Google Play Protect.

Příklady porušení zásad:

- Shromažďování dat (srov. Spyware)
- Zneužití omezených oprávnění

Příklady zásad pro údaje o uživatelích:

- Zásady služby Google Play pro údaje o uživatelích
- Zásady pro údaje o uživatelích v požadavcích Služeb Google pro mobily
- Zásady služby Google API pro údaje o uživatelích

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

Nepřátelské stahovací programy

Kód, který není nežádoucím softwarem, ale stahuje jiný nežádoucí software pro mobilní zařízení.

O nepřátelské stahování se může jednat za těchto podmínek:

- existuje důvodné přesvědčení, že kód byl vytvořen za účelem šíření nežádoucího softwaru pro mobilní zařízení a stáhl nějaký nežádoucí software pro mobilní zařízení nebo obsahuje kód, který by mohl stahovat a instalovat aplikace, nebo
- minimálně 5 % aplikací stažených prostřednictvím kódu jsou nežádoucím softwarem pro mobilní zařízení, přičemž platí minimální hranice 500 zjištěných stažených aplikací (tj. 25 zjištěných stažení nežádoucího softwaru pro mobilní zařízení).

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

- nespouštějí stahování bez interakce uživatele a
- veškeré stahování softwaru je iniciováno souhlasem uživatele.

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 inzerenty, vývojáře a uživatele škodlivé a vedou k dlouhodobé ztrátě důvěry v ekosystém mobilních reklam.

Příklady běžných porušení zásad:

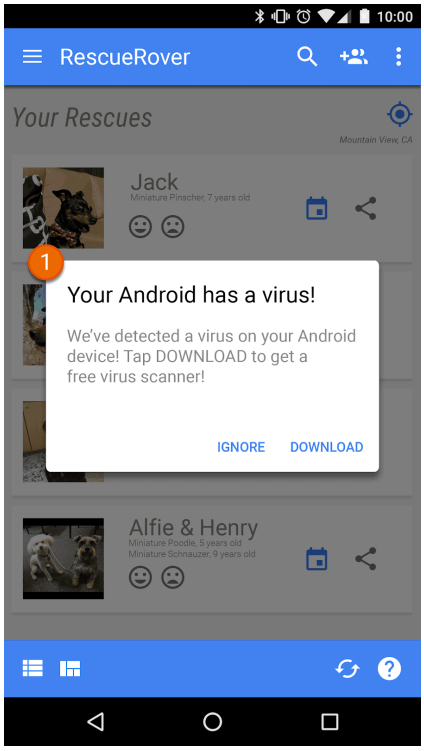
- Aplikace zobrazující reklamy, které nejsou pro uživatele viditelné.
- Aplikace, která bez záměru uživatele automaticky generuje kliknutí na reklamy nebo která generuje ekvivalentní síťový provoz za účelem podvodného přiřazení kreditů za kliknutí.
- Aplikace odesílající falešná kliknutí na atribuci instalace, aby dostala zaplaceno 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, 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.

Sociální inženýrství

Nepovolujeme aplikace, které se vydávají za jinou aplikaci s cílem přimět uživatele k provedení akcí, které měl uživatel v úmyslu provést v původní důvěryhodné aplikaci.

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. Protože 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 pro tyto transakce používat fakturační systém služby Google Play.
2. Aplikace distribuované na Google Play, které vyžadují nebo přijímají platby za přístup ke svým funkcím nebo službám (včetně funkcí aplikace, digitálního obsahu nebo zboží, souhrnně „nákupy v aplikaci“), musí pro tyto transakce používat fakturační systém Google Play. Výjimku tvoří případy popsané v oddílech 3, 8 a 9.

   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, upgrady služby nebo jiné služby s předplaceným obsahem),
- funkce nebo obsah aplikace (např. verze aplikace bez reklam nebo nové funkce, které verze za 0 Kč nenabízí),
- cloudový software a služby (například služby úložiště dat, software pro zvýšení firemní produktivity nebo software pro správu financí).

3. Fakturační systém služby Google Play nesmí být používán v případech, kdy:
   a. je platba primárně určena:
      - 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),
   b. platby zahrnují peer-to-peer platby, úhrady online aukcí nebo dary osvobozené od daní,
   c. platba je za obsah či služby, které zpřístupňují online hazard, jak je popsáno v oddílu Hazardní aplikace v zásadách her, soutěží a hazardních her se skutečnými penězi,
   d. platba se týká kategorie produktů, která je podle obsahových zásad centra plateb Google považována za nepřijatelnou.

      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 .

4. Kromě případů popsaných v oddílech 3, 8 a 9 nesmí aplikace uživatele navádět na jinou platební metodu, než je 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 prodávaným 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 přesměrovávají z aplikace k jiné platební metodě, než je fakturační systém služby Google Play.
5. Virtuální měny v aplikacích smí být používány pouze v aplikaci nebo hře, ve které byly koupeny.
6. 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.
7. Aplikace a hry, které umožňují nákupy náhodných virtuálních položek (mimo jiné tzv. loot boxy), musí před nákupem jasně a včasně informovat o pravděpodobnosti získání takových položek.
8. Pokud neplatí podmínky popsané v oddílu 3, vývojáři aplikací distribuovaných na Google Play, které za účelem přístupu k nákupům v aplikaci vyžadují nebo přijímají platby od uživatelů z těchto zemí/oblastí, mohou uživatelům pro tyto transakce kromě fakturačního systému Google Play nabízet také alternativní fakturační systém v aplikaci. Podmínkou je, že tito vývojáři vyplní formulář deklarace jiného fakturačního systému pro příslušný program a vyjádří souhlas s dodatečnými smluvními podmínkami a programovými požadavky zahrnutými v tomto formuláři.
9. Uživatele z Evropského hospodářského prostoru (EHP) mohou vývojáři aplikací distribuovaných na Google Play přesměrovat mimo aplikaci mimo jiné za účelem propagace nabídek digitálních funkcí a služeb v aplikaci. Vývojáři, kteří uživatele z EHP přesměrovávají mimo aplikaci, musí vyplnit formulář

deklarace pro tento program a odsouhlasit dodatečné smluvní podmínky a požadavky programu zahrnuté v tomto formuláři.

Poznámka: Časové osy a časté dotazy týkající se těchto zásad naleznete v centru nápovědy.

Reklamy

Za účelem zajišťování kvalitních služeb bereme v potaz obsah reklamy, publikum, uživatelský dojem, chování, zabezpečení a ochranu soukromí. Reklamy a související nabídky považujeme za součást vaší aplikace, musí proto dodržovat všechny další zásady Google Play. Pokud zpeněžujete aplikaci, která na Google Play cílí na děti, na obsažené reklamy se vztahují další požadavky.

Další informace o zásadách pro propagaci aplikace a záznamy v obchodu si můžete přečíst tady, včetně toho, jak reagujeme na podvodné propagační praktiky.

Obsah reklamy

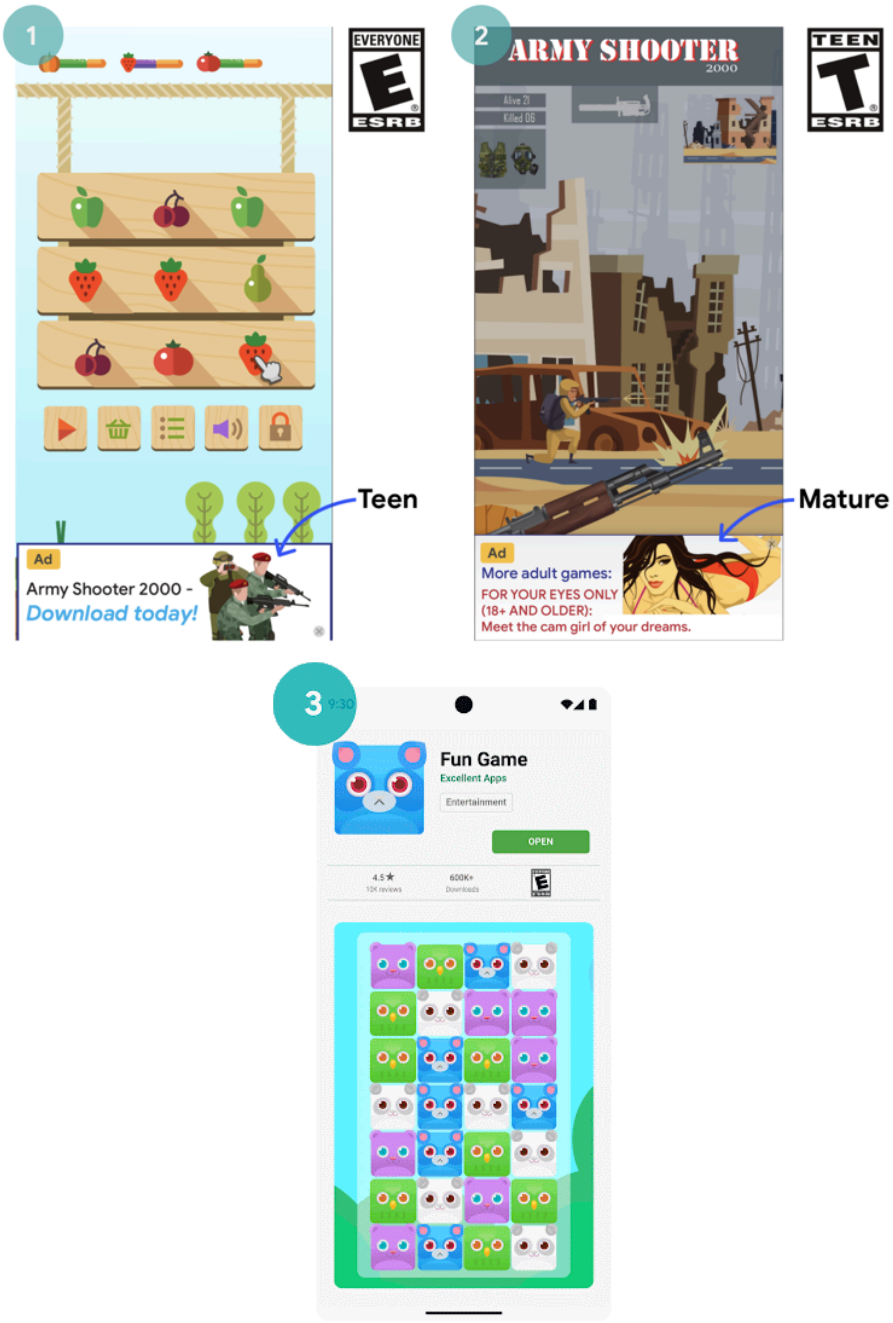
Reklamy a související nabídky musí být součástí vaší aplikace a musí splňovat zásady ohledně omezeného obsahu. Další požadavky platí, pokud je vaše aplikace hazardní.

Nevhodné reklamy

Reklamy a související nabídky (například reklama propagující stažení jiné aplikace) zobrazené v aplikaci musí odpovídat hodnocení obsahu aplikace, i když obsah sám o sobě je jinak v souladu s našimi zásadami.

Příklady běžných porušení zásad:

- Reklamy, které nejsou vhodné pro hodnocení obsahu aplikace



① Tato reklama (pro mládež) není vhodná pro hodnocení obsahu aplikace (všichni)
② Tato reklama (pro dospělé) není vhodná pro hodnocení obsahu aplikace (pro mládež)
③ Nabídka reklamy (propagující stažení aplikace pro dospělé) není vhodná pro hodnocení obsahu herní aplikace, ve které byla zobrazena (Všichni)

Požadavky na reklamy pro rodiny

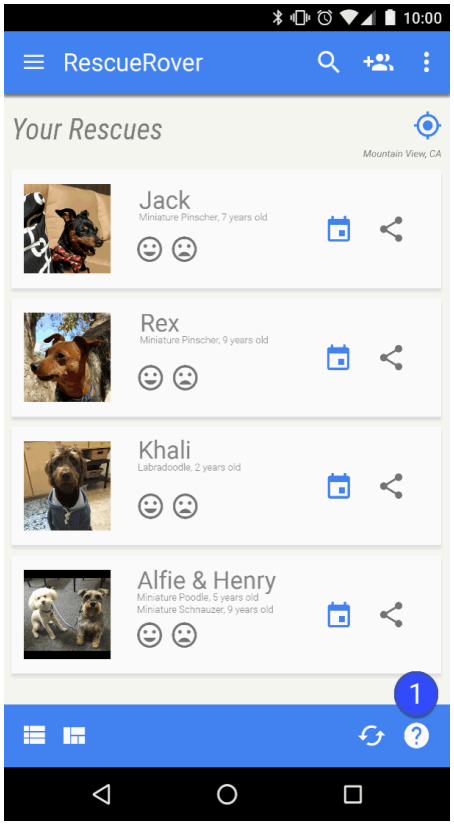
Pokud zpeněžujete aplikaci, která ve službě Play cílí na děti, aplikace musí splňovat zásady ohledně reklam a zpeněžování obsahu pro rodiny.

Klamavé reklamy

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

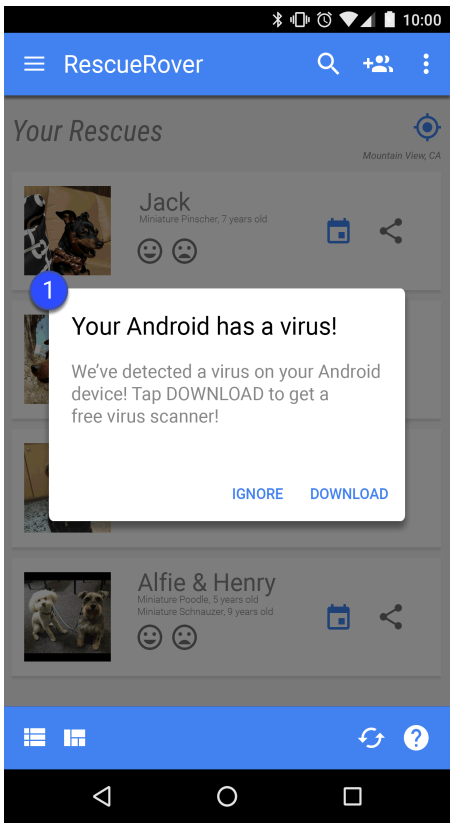
Příklady běžných porušení zásad:

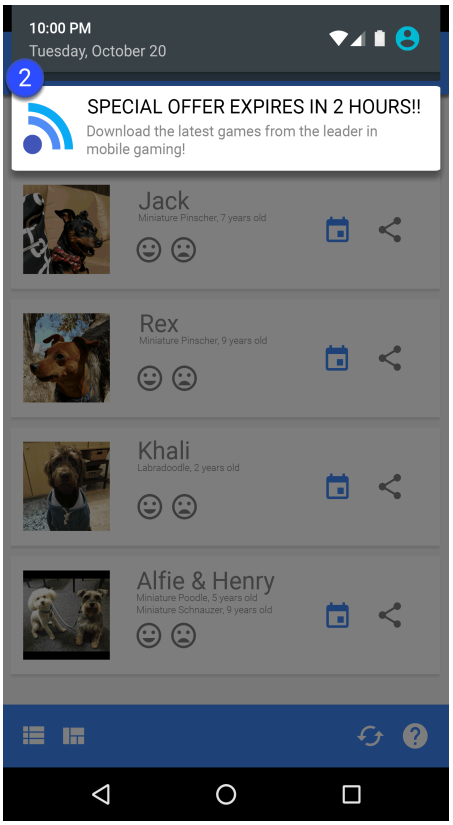
- Reklamy, které napodobují uživatelské rozhraní aplikace:



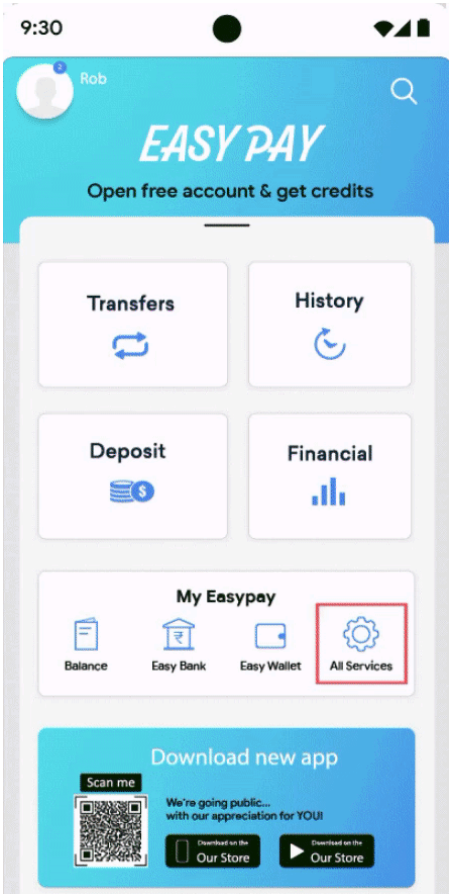
① Ikona otazníku v této aplikaci je reklama, která uživatele přesměrovává na externí vstupní stránku.

- Reklamy, které napodobují systémová oznámení:





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



① Výše uvedený příklad ilustruje sekci funkcí, která napodobuje jiné funkce, ale vede uživatele pouze k reklamám.

Rušivé reklamy

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

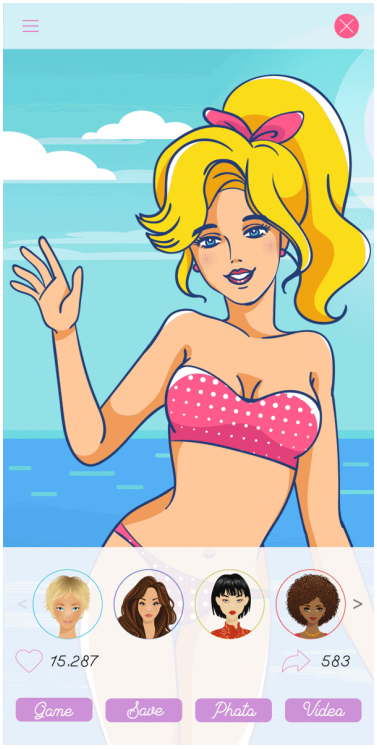
Aplikace nesmí uživatele nutit, aby dříve, než bude moci aplikaci plně používat, klikal na reklamu nebo odesílal osobní údaje k reklamním účelům. Reklamy se mohou zobrazovat pouze v aplikaci, která jejich zobrazení realizuje. Nesmí rušit ostatní aplikace, reklamy nebo fungování zařízení, včetně systému a tlačítek a portů zařízení. To zahrnuje překryvné reklamy, funkce doprovodné reklamy i reklamní jednotky v podobě widgetů. Pokud aplikace zobrazuje obsahové nebo jiné reklamy, které narušují běžnou práci s aplikací, musíte uživateli umožnit tyto reklamy snadno zavřít bez jakékoli penalizace.

Příklady běžných porušení zásad:

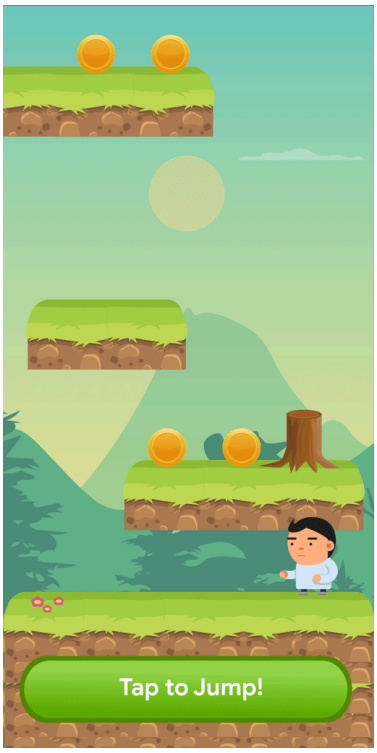
- Reklama, která zabere celou obrazovku nebo jinak brání běžné práci s aplikací a neposkytuje jasně viditelnou možnost reklamu zavřít:

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:

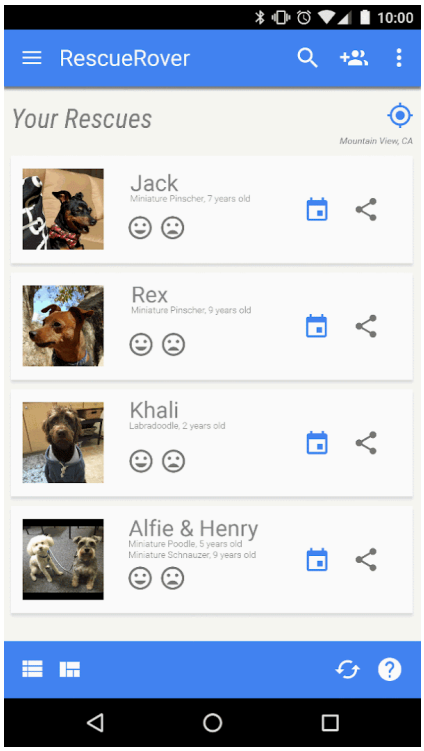


① Tato reklama používá falešné tlačítko pro zavření.



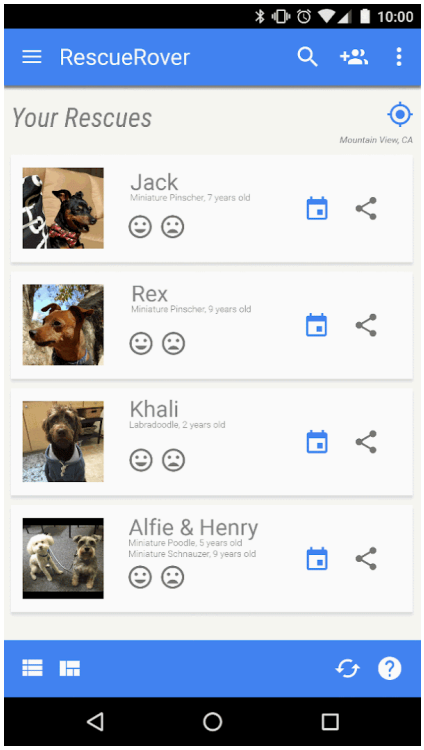
② Tato reklama se náhle zobrazí v oblasti, kde uživatel obvykle klepá na jinou funkci aplikace.

- Reklamy zobrazované mimo aplikaci, která zobrazení realizuje:



① 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:



① Uživatel se snaží aplikaci opustit a přejít na plochu, ale očekávaný průběh této operace je narušen reklamou.

Lepší dojem z reklamy

Kvůli zajištění kvalitního uživatelského dojmu při používání aplikací z Google Play jsou vývojáři povinni dodržovat následující pokyny pro reklamy. Reklamy se uživatelům nesmějí zobrazovat následujícími neočekávanými způsoby:

- Nejsou povoleny vsunuté reklamy na celou obrazovku všech formátů (video, GIF, statické apod.), které se zobrazují neočekávaně, obvykle když se uživatel rozhodne udělat něco jiného.
  - Nejsou povoleny reklamy, které se objevují během hraní hry na začátku úrovně nebo na začátku segmentu obsahu.
  - Nejsou povoleny vsunuté videoreklamy na celou obrazovku, které se zobrazují před obrazovkou načítání aplikace (před úvodní obrazovkou).
- Nejsou povoleny vsunuté reklamy na celou obrazovku všech formátů, které nelze zavřít po 15 sekundách. Vsunuté reklamy na celou obrazovku, k jejichž zobrazování se uživatelé výslovně přihlásili, nebo vsunuté reklamy na celou obrazovku, které uživatele nepřerušují v akci (například po obrazovce se skóre v herní aplikaci), mohou přetrvávat déle než 15 sekund.

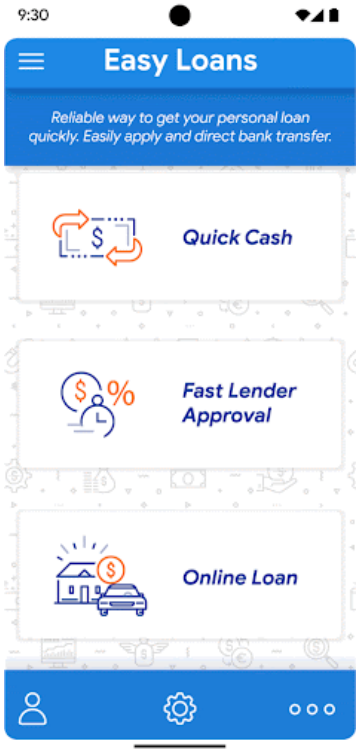
Tyto zásady se nevztahují na reklamy s nabídkou odměny, ke kterým se uživatelé výslovně přihlásili (například reklama, jejíž zhlédnutí vývojáři uživateli nabízejí výměnou za odemknutí konkrétní herní funkce nebo obsahu). Tyto zásady se také nevztahují na zpeněžování a reklamu, které nenarušují běžné používání aplikací nebo hraní her (například videoobsah s integrovanými reklamami, bannerové reklamy, které nezabírají celou obrazovku).

Tyto pokyny vycházejí z pokynů pro prostředí mobilních aplikací ve standardech pro lepší reklamy . Další informace o standardech pro lepší reklamy najdete na webu Koalice za lepší reklamy .

Příklady běžných porušení zásad:

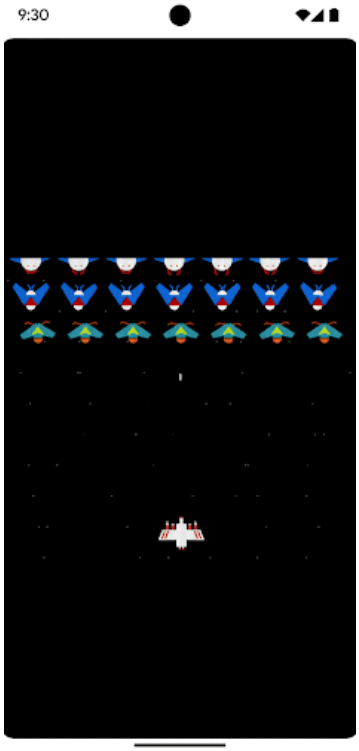
- Neočekávané reklamy, které se objevují během hraní hry nebo na začátku segmentu obsahu (například poté, co uživatel klikne na tlačítko, ale předtím, než se projeví zamýšlená akce tlačítka). Tyto reklamy jsou pro uživatele neočekávané, protože uživatelé očekávají, že místo nich začne hra nebo obsah.

① Během hraní hry se na začátku úrovně objeví neočekávaná statická reklama.



② Na začátku segmentu obsahu se objeví neočekávaná videoreklama.

- Celoobrazovková reklama, která se zobrazuje během hraní hry a kterou nelze zavřít po 15 sekundách.



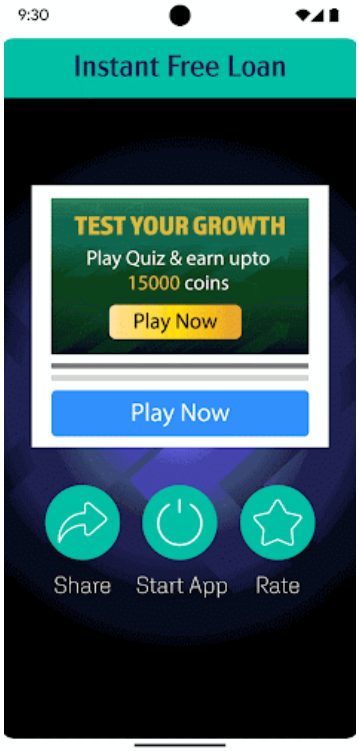
① Během hraní hry se zobrazuje vsunutá reklama, která uživatelům během 15 sekund nenabízí možnost zavření.

Vytvořeno pro reklamy

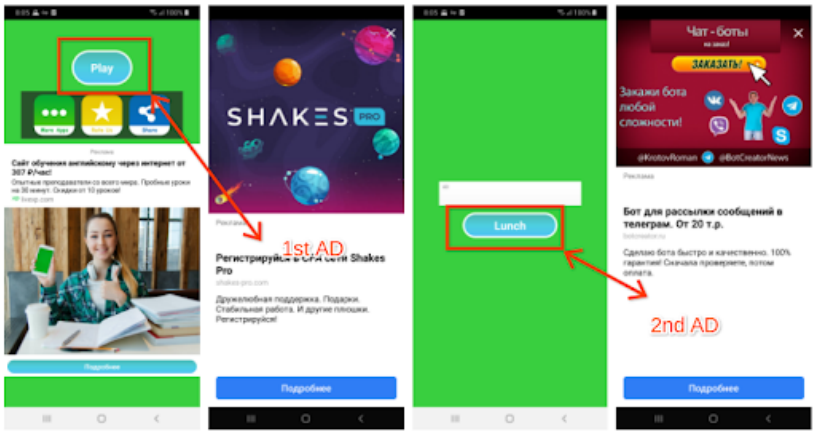
Nepovolujeme aplikace, které opakovaně zobrazují vsunuté reklamy, a odvádějí tak pozornost uživatelů od interakce s aplikací a provádění úkolů v aplikaci.

Příklady běžných porušení zásad:

- Aplikace, ve kterých se po akcích uživatele (například po kliknutí, přejetí prstem apod.) soustavně zobrazují vsunuté reklamy.



① Na první stránce aplikace je několik tlačítek, se kterými lze pracovat. Když uživatel za účelem použití aplikace klikne na **Spustit aplikaci**, zobrazí se vsunutá reklama. Po zavření reklamy se uživatel vrátí do aplikace a klikne na **Služba**, aby začal používat službu, ale zobrazí se další vsunutá reklama.



② Na první stránce uživatel musí kliknout na tlačítko **Hrát**, protože to je jediné dostupné tlačítko k použití aplikace. Když na něj uživatel klikne, zobrazí se vsunutá reklama. Po zavření reklamy uživatel klikne na **Spustit**, protože je to jediné tlačítko, se kterým lze interagovat, a zobrazí se další vsunutá reklama.

Zpeněžení obrazovky uzamčení

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

Inzertní podvody

Inzertní podvody jsou přísně zakázány. Další informace naleznete v zásadách ohledně inzertních podvodů.

Používání údajů o poloze pro reklamy

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

- O používání nebo shromažďování údajů o poloze zařízení chráněných oprávněním k inzertním účelům musí být uživatel informován a musí být zdokumentováno v povinných zásadách ochrany soukromí aplikace, a to včetně odkazu na zásady ochrany soukromí reklamní sítě, které se týkají používání údajů o poloze.
- V souladu s požadavky na oprávnění pro přístup k poloze je o toto oprávnění dovoleno žádat pouze za účelem implementace aktuálních funkcí nebo služeb aplikace. O toto oprávnění není dovoleno žádat výhradně pro účely zobrazování reklam.

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 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 není dovoleno pro účely analýzy přidružit k informacím, které umožňují zjištění totožnosti, ani k trvalému identifikátoru zařízení (např. SSAID, adresa MAC, číslo IMEI apod.). Další pokyny ohledně trvalých identifikátorů zařízení naleznete v zásadách pro údaje o uživatelích .
- **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.
  - 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.
  - Když na novějších zařízeních uživatel inzertní identifikátor Android smaže, identifikátor bude odstraněn. Při pokusu o získání identifikátoru bude vrácen řetězec nul. Zařízení bez inzertního identifikátoru nesmí být propojeno s daty, která byla získána nebo odvozena z předchozího identifikátoru.
- **Transparentnost pro uživatele**. Uživatelé musejí být o shromažďování a využití reklamního identifikátoru a závazku dodržovat tyto smluvní podmínky informováni v právně přiměřeném oznámení o ochraně soukromí. Další informace o standardech ochrany soukromí naleznete v článku o zásadách týkajících se údajů o uživateli .
- **Dodržování smluvních podmínek**. Inzertní identifikátor je dovoleno používat pouze v souladu s programovými zásadami služby Google Play pro vývojáře. Tyto zásady 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).

Další informace naleznete v zásadách pro údaje o uživatelích.

Odběry

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. Nepovolujeme aplikace, které uživatele vystavují podvodným nebo manipulativním nákupům (včetně nákupů v aplikaci nebo předplatného).

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.

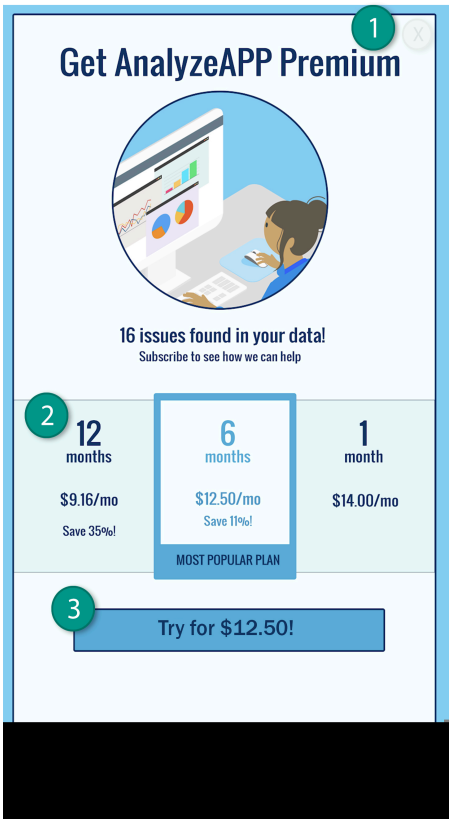
Předplatné musí uživatelům poskytovat trvalou nebo opakující se hodnotu po celou dobu trvání předplatného a nesmí být používáno k nabízení jednorázových výhod (například jednotky SKU, které poskytují jednorázové kredity/peníze v aplikaci nebo herní boostery na jedno použití). Vaše předplatné může nabízet motivační nebo propagační bonusy, které však musí doplňovat trvalou nebo opakující se hodnotu poskytovanou po celou dobu trvání předplatného. Produkty, které nenabízejí trvalou nebo opakující se hodnotu, musí být označeny jako produkt v aplikaci a ne jako předplatné.

Jednorázové výhody pro uživatele nesmíte maskovat nebo nesprávně charakterizovat jako předplatné. To zahrnuje úpravu předplatného tak, aby se z něj stala jednorázová nabídka (například zrušení, ukončení podpory nebo minimalizace opakující se hodnoty) poté, co uživatel předplatné zakoupil.

Příklady běžných porušení zásad:

- Měsíční předplatné uživatele neinformuje o tom, že se bude každý měsíc automaticky obnovovat a strhávat platba.
- Roční předplatné nejvýrazněji zobrazuje 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“ nebo „Vyzkoušejte prémiové členství – 3 dny zdarma“, ačkoliv jsou za něj automaticky účtovány pravidelné platby).
- Několik obrazovek v procesu nákupu vede uživatele k náhodnému kliknutí na tlačítko předplatného.
- Předplatné, které nenabízí trvalou nebo opakující se hodnotu – například nabídka 1 000 drahokamů za první měsíc, ale poté jen 1 drahokam měsíčně.
- Požadavek, aby se uživatel zaregistroval k automatickému obnovování předplatného za účelem poskytnutí jednorázové výhody, a zrušení předplatného uživatele bez jeho žádosti po nákupu.

Příklad 1:



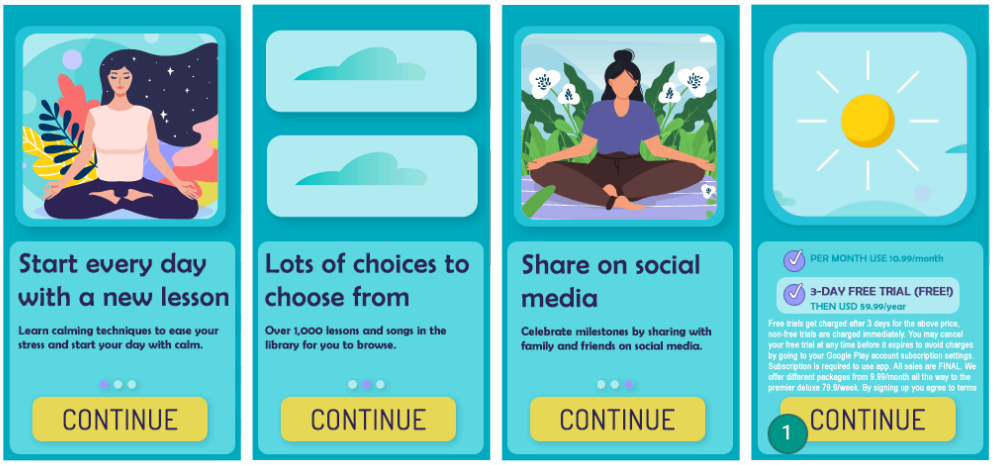
① Není zobrazeno tlačítko k odmítnutí a uživatelům nemusí být jasné, že funkce mohou používat i bez přijetí nabídky předplatného.

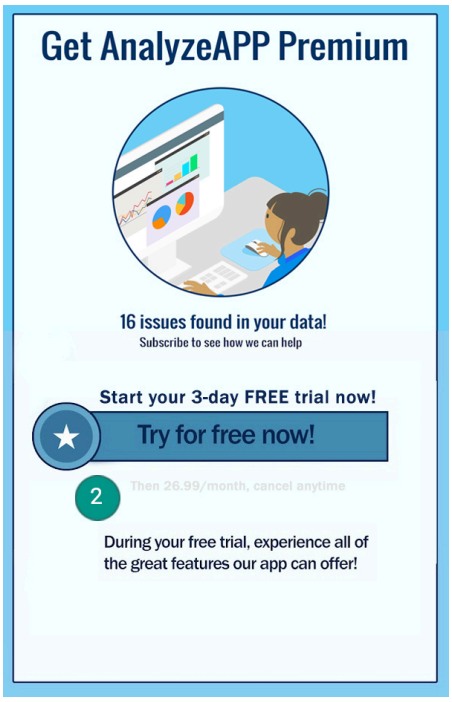
② V nabídce je uvedena pouze cena za měsíc a uživatelům nemusí být jasné, že jim při přihlášení k odběru bude naúčtována cena za šest měsíců.

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.

Příklad 2:





① Opakovaná kliknutí na stejnou oblast tlačítka způsobí, že uživatel neúmyslně klikne na konečné tlačítko pro pokračování na předplatné.

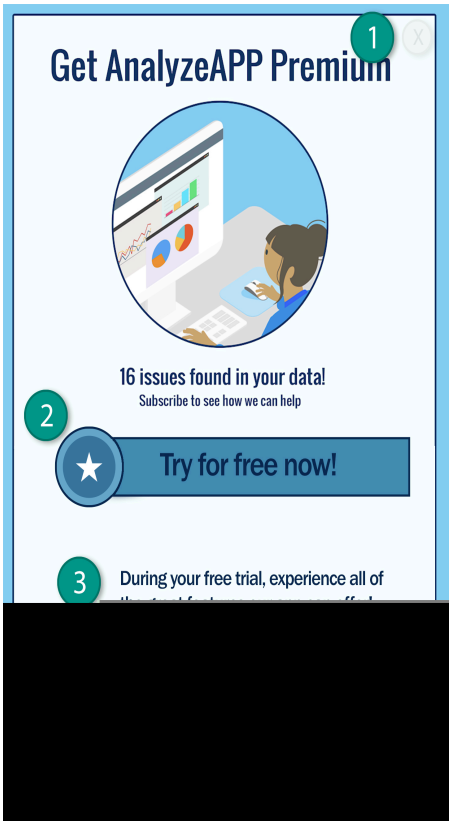
② Částku, která je uživatelům účtována na konci zkušebního období, lze jen těžko přečíst, a proto se uživatelé mohou domnívat, že se jedná o bezplatný tarif

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 předplatných, zrušení a vracení peněz

Pokud ve svých aplikacích prodáváte předplatné, musíte v nich jasně uvést, jak uživatelé své předplatné mohou spravovat nebo zrušit. Aplikace také musí zahrnovat přístup ke snadno použitelné online metodě zrušení předplatného. V nastavení účtu aplikace (nebo na podobné stránce) můžete tento požadavek splnit tím, že zahrnete:

- odkaz na centrum předplatných Google Play (pro aplikace, které používají fakturační systém služby Google Play) a/nebo
- přímý přístup k vašemu procesu zrušení

Pokud uživatel zruší předplatné zakoupené prostřednictvím fakturačního systému služby Google Play, podle našich zásad takovému uživateli nebude vrácena platba za aktuální fakturační období, ale bez ohledu na datum zrušení bude po zbytek aktuálního fakturačního období i nadále dostávat předplacený obsah. Předplatné bude zrušeno po skončení aktuálního fakturačního období.

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

Program sad SDK pro reklamy s vlastní certifikací pro rodiny

Pokud v aplikaci zobrazujete reklamy a cílovým publikem jsou pouze děti (jak je popsáno v zásadách pro rodiny), smíte použít pouze sady SDK pro reklamy, které mají vlastní certifikaci v souladu se zásadami služby Google Play, včetně splnění níže uvedených požadavků na sady SDK pro reklamy s vlastní certifikací pro rodiny.

Pokud vaše aplikace cílí na děti i starší uživatele, musíte zajistit, aby reklamy zobrazované dětem pocházely výhradně z některé z těchto verzí sad SDK pro reklamy s vlastní certifikací (například pomocí neutrálního věkového filtru).

Je vaší odpovědností zajistit, aby všechny verze sad SDK implementované v aplikaci, včetně verzí sad SDK pro reklamy s vlastní certifikací, vyhovovaly všem příslušným zásadám, místním zákonům a jiným právním předpisům. Google nepotvrzuje ani nezaručuje přesnost informací, které sady SDK pro reklamy poskytnou v rámci procesu vlastní certifikace.

Použití sad SDK pro reklamy s vlastní certifikací pro rodiny je povinné pouze v případě, že je používáte k zobrazování reklam dětem. Následující možnosti jsou povoleny bez vlastní certifikace sady SDK pro reklamy u Google Play, avšak nadále nesete odpovědnost za to, že reklamní obsah a postupy shromažďování údajů budou v souladu se zásadami pro údaje o uživatelích a se zásadami pro rodiny služby Google 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 sady SDK pro reklamy s vlastní certifikací pro rodiny

- Definujte nevhodný obsah a chování reklam a ve smluvních podmínkách a zásadách sady SDK pro reklamy je zakažte. Definice musí splňovat programové zásady služby Google Play pro vývojáře.
- Vytvořte metodu k hodnocení kreativ 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 sad SDK pro reklamy určených pro děti byly deaktivovány personalizované reklamy, zájmově orientované reklamy a remarketing.
- Vydavatelé 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. odesláním testovací aplikace a informací ve formuláři pro zájemce uvedeném níže), aby mohla ověřit, zda sada SDK pro reklamy splňuje všechny požadavky na vlastní certifikaci, včas odpovídejte na všechny následné žádosti o informace, jako je odeslání nové verze za účelem ověření souladu sady SDK pro reklamy se všemi požadavky na vlastní certifikaci, a poskytněte testovací aplikaci.
- Sami potvrďte , že jsou všechny nové verze v souladu s nejnovějšími programovými zásadami služby Google Play pro vývojáře, včetně požadavků zásad pro rodiny.

Poznámka: Sady SDK pro reklamy s vlastní certifikací pro rodiny musejí podporovat zobrazování reklam, které je v souladu se všemi relevantními předpisy a nařízeními ohledně dětí, jež se na majitele obsahu mohou vztahovat.

Další informace o označení reklamních kreativ vodoznakem a poskytnutí testovací aplikace najdete zde .

Požadavky na zprostředkování pro reklamní platformy při zobrazování reklam dětem:

- Používejte pouze sady SDK pro reklamy s vlastní certifikací pro rodiny 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.

Seznam sad SDK pro reklamy s vlastní certifikací pro rodiny a informace o tom, které konkrétní verze těchto sad SDK pro reklamy mají vlastní certifikaci k použití v aplikacích pro rodiny, najdou vývojáři zde .

Poskytovatele sad SDK pro reklamy, 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 (např. reklamy), které klamou nebo škodí uživatelům či vývojářskému ekosystému. Propagační praktiky jsou považovány za klamavé nebo škodlivé, pokud jejich chování nebo obsah porušuje naše programové zásady pro vývojáře.

Příklady běžných porušení zásad:

- používání klamavých reklam na webech, v aplikacích nebo jiných službách, včetně oznámení, která připomínají systémová oznámení či upozornění,
- používání sexuálně explicitních reklam k přesměrování uživatelů do vašeho záznamu na Google Play za účelem stažení aplikace,
- propagační nebo instalační taktiky, které uživatele přesměrovávají na Google Play nebo spouštějí stahování aplikací bez vědomé akce uživatele,
- nevyžádaná propagace prostřednictvím zpráv SMS,
- text nebo obrázky v názvu či ikoně aplikace nebo v názvu vývojáře, které obsahují tvrzení o výkonu nebo hodnocení v obchodu, propagační informace nebo tvrzení o vztahu s programy Google Play.

Je vaší povinností zajistit, aby reklamní sítě, spřízněné subjekty a reklamy přidružené k aplikaci tyto zásady dodržovaly.

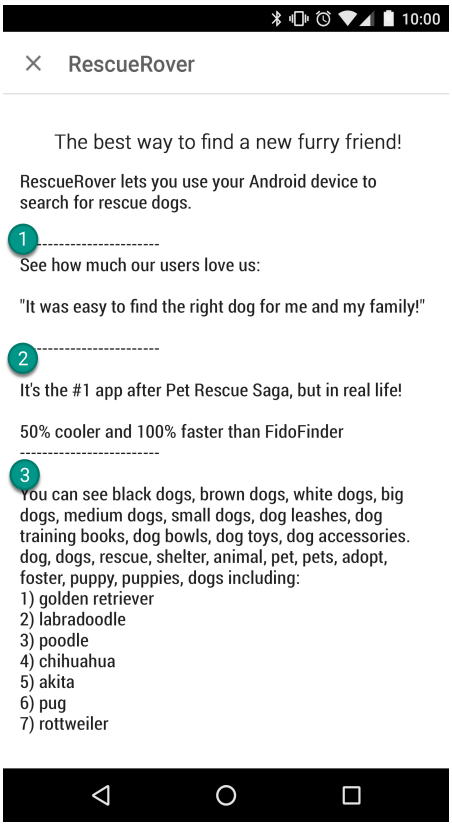
Metadata

Popisy uživatelům umožňují zjistit, jaké funkce vaše aplikace poskytuje a k čemu slouží. 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 prohlášení uživatelů.

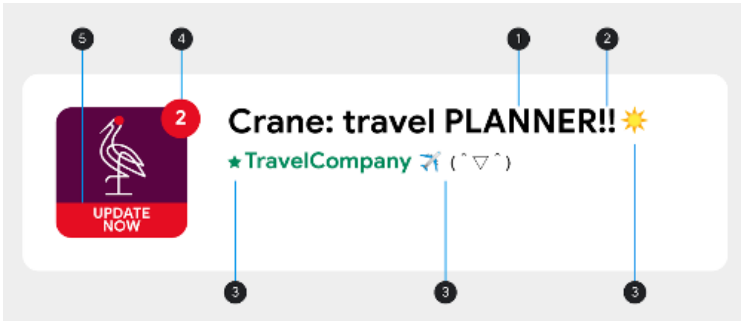
Uživatelé vaši aplikaci nejlépe najdou a poznají podle názvu a ikony a podle jména vývojáře. V těchto prvcích metadat nepoužívejte smajlíky ani opakované speciální znaky. Nepište názvy VELKÝMI PÍSMENY, leda by šlo o součást názvu vaší značky. V ikonách aplikací nejsou dovoleny zavádějící symboly, např. puntík označující novou zprávu, když žádná zpráva nepřišla, nebo symbol stažení či instalace, když aplikace nesouvisí se stahováním obsahu. Název aplikace smí mít maximálně 30 znaků. V názvu aplikace, ikoně či jménu vývojáře nepoužívejte text ani obrázky, které obsahují tvrzení o výkonu nebo hodnocení v obchodu, propagační informace nebo tvrzení o vztahu s programy Google Play.

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

Příklady běžných porušení zásad:

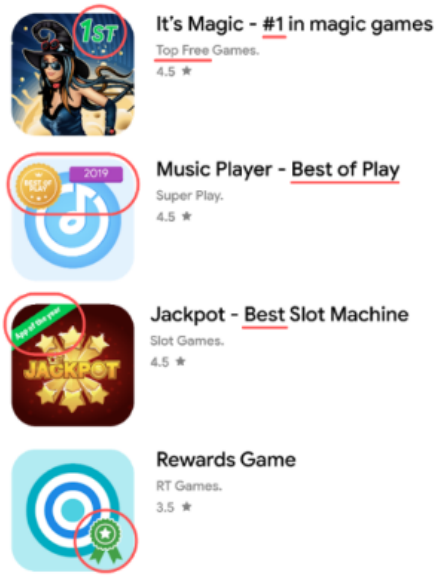


① Anonymní nebo nepřiřazená prohlášení uživatelů
② Porovnání dat aplikací nebo značek
③ Bloky slov nebo vertikální či horizontální seznamy slov

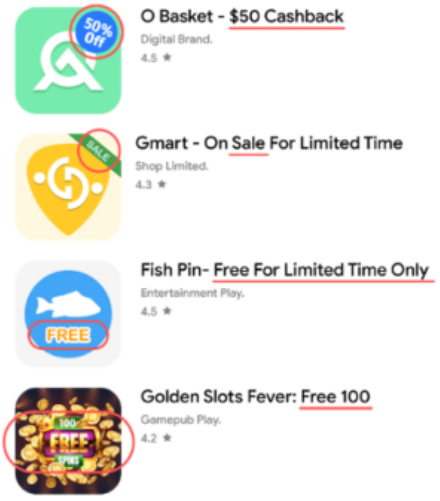


① Název VELKÝMI PÍSMENY, pokud se nejedná o součást názvu značky
② Sekvence speciálních znaků nerelevantních pro značku
③ Smajlíky a speciální znaky
④ Zavádějící symboly
⑤ Zavádějící text

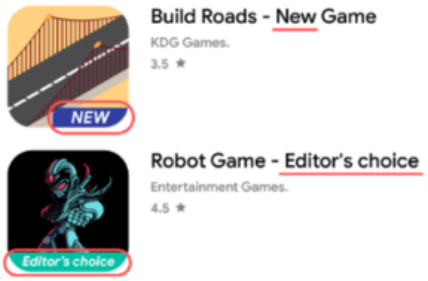
- Obrázky nebo text, které uvádějí výkon nebo hodnocení v obchodu, např. Nejlepší apka roku, Jednička na trhu, To nejlepší na Google Play za rok 20XX, Oblíbené, ikony ocenění apod.



- Obrázky nebo text, které uvádějí cenu nebo propagační informace, např. Sleva 10 %, Cashback 50 $, Po omezenou dobu zdarma apod.



- Obrázky nebo text, které uvádějí programy služby Google Play, např. Výběr redakce, Novinka apod.



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

- Obrázky nebo videa se sexuálním podtextem. Nepoužívejte reálné ani ilustrované obrázky se sexuálním podtextem, které vyobrazují ňadra, hýždě, genitálie ani jiné části těla či obsah, který může být předmětem sexuálního vzrušení.
- Vulgární, neslušné a jiné výrazy, které nejsou vhodné pro obecné publikum.
- Názorné násilí nápadně vyobrazené v ikonách aplikace, propagačních obrázcích či videích.
- Vyobrazení nezákonné konzumace drog. Také obsah vzdělávacího, dokumentárního, vědeckého nebo uměleckého charakteru v záznamu v obchodu musí být vhodný pro všechny kategorie publika.

Zde je několik doporučených postupů:

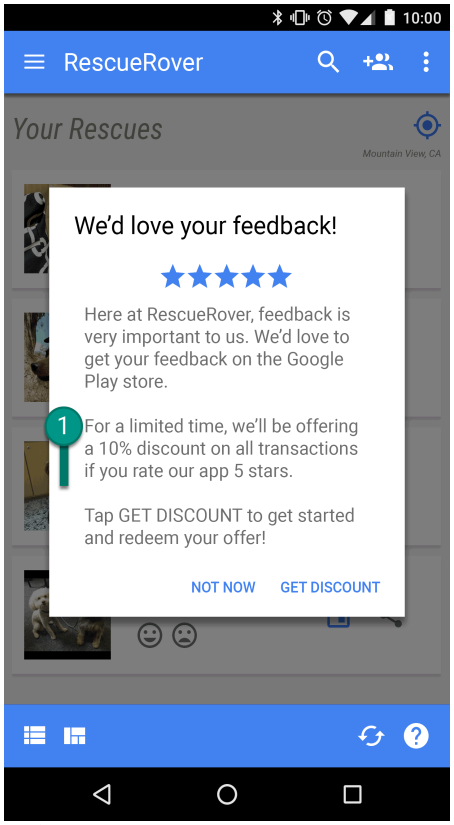
- Zdůrazněte, co je na vaší aplikaci skvělého. Podělte se s uživateli o zajímavá a poutavá fakta, aby vaši aplikaci snáze odlišili od konkurence.
- Název a popis aplikace musí přesně popisovat její funkce.
- Nepoužívejte opakující se ani nesouvisející klíčová slova a reference.
- Popis aplikace by měl 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. Jsou zakázány také aplikace, jejichž hlavní funkcí je pobídkami uživatele motivovat k instalaci jiných aplikací.

Příklady běžných porušení zásad:

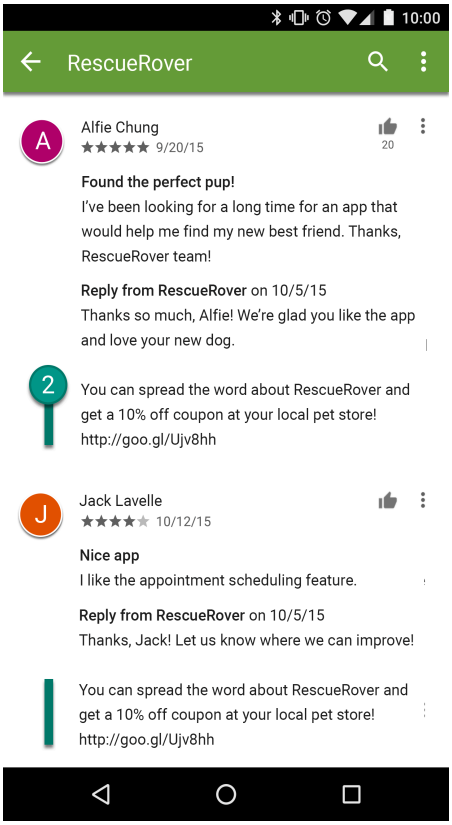
- Nabízení odměn za hodnocení aplikace:



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

- Opakované odesílání hodnocení vydávajících se za uživatele s cílem ovlivnit umístění aplikace na Google Play.

- Odesílání recenzí s nevhodným obsahem (např. s odkazy na partnery, kupóny, herními kódy, e-mailovými adresami nebo odkazy na weby či jiné aplikace) nebo vybízení uživatelů k takovému jednání:



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

Hodnocení a recenze slouží jako ukazatele kvality aplikace. Uživatelé se spoléhají, že budou autentické 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 hodnoticích orgánů. Chybný popis obsahu aplikace může vést k odstranění nebo pozastavení aplikace. Proto je důležité, abyste v dotazníku hodnocení obsahu odpovídali přesně.

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

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

Další informace o různých hodnoticích orgánech a pokyny k vyplnění dotazníku hodnocení obsahu naleznete v centru nápovědy .

Odvolání proti hodnocení

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

Zprávy

Zpravodajská aplikace musí splňovat tato kritéria:

- v Google Play Console sama sebe deklaruje jako zpravodajská, nebo
- na Google Play je uvedena v kategorii Noviny a časopisy a definuje se jako zpravodajská v názvu, ikoně, jménu vývojáře nebo popisu.

Příklady aplikací v kategorii Noviny a časopisy, které se kvalifikují jako zpravodajské:

- Aplikace, které v popisu zmiňují zpravodajství, například:
  - Nejnovější zprávy
  - Noviny
  - Mimořádné zprávy
  - Místní zprávy
  - Denní zprávy
- Aplikace, které zmiňují zprávy ve svém názvu, ikoně nebo jménu vývojáře.

Pokud ale aplikace primárně zahrnuje obsah generovaný uživateli (např. sociální média), nesmí se deklarovat jako zpravodajská a nebude považována za zpravodajskou.

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

Zpravodajské aplikace musí:

- Poskytnout informace o vlastnictví – o aplikaci a zdroji zpravodajských článků (mimo jiné původní vydavatel nebo autor každého článku). Pokud není zvykem uvádět jednotlivé autory článků, zpravodajská aplikace musí být původním vydavatelem článků. Upozorňujeme, že odkazy na účty na sociálních sítích jako údaje o autorovi nebo vydavateli nestačí.
- Mít vyhrazené webové stránky nebo stránku v aplikaci pro kontaktní údaje, které budou jasně označené, snadno dostupné (např. prostřednictvím odkazu ve spodní části domovské stránky nebo v postranním navigačním panelu) a budou obsahovat platné kontaktní údaje vydavatele zpráv, buď kontaktní e-mailovou adresu, nebo telefonní číslo.Upozorňujeme, že odkazy na účty na sociálních sítích jako kontaktní údaje vydavatele nestačí.

Zpravodajské aplikace nesmí:

- Obsahovat výrazné gramatické a pravopisné chyby.

- Obsahovat výhradně statický obsah (např. obsah starý více než tři měsíce).
- Mít jako hlavní účel affiliate marketing nebo tržby z reklam.

Upozorňujeme, že zpravodajské aplikace *smějí* za účelem zpeněžení používat reklamy a další formy marketingu pod podmínkou, že primárním účelem aplikace není prodej produktů a služeb nebo generování výnosů 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.

Pokyny, jak nejlépe poskytnout požadované informace, naleznete v tomto článku .

Spam, funkčnost a uživatelský dojem

Aplikace musí uživatelům poskytovat základní úroveň adekvátní funkčnosti a obsahu, aby pro uživatele byly přínosné. 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.

Příklad běžného porušení zásad:

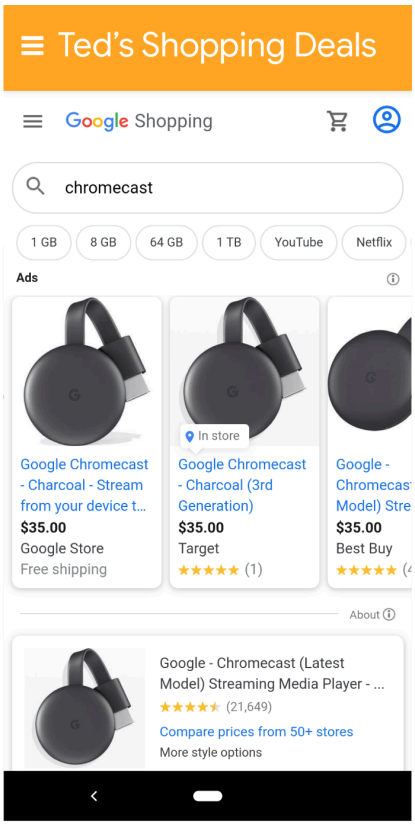
- Když uživatel použije tlačítko Sdílet, aplikace odešle jeho jménem zprávy, aniž by uživatel mohl potvrdit obsah a příjemce:

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 poskytovat zobrazení webu bez svolení:



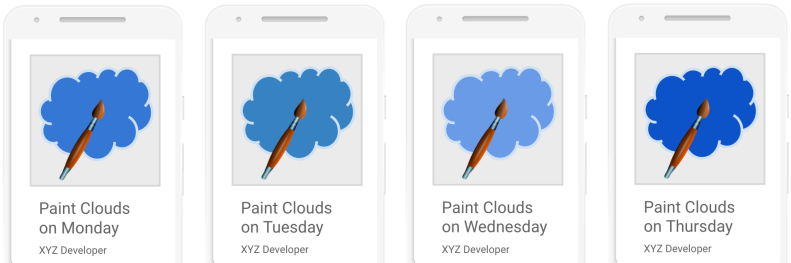
① Tato aplikace se nazývá „Tedovy nákupní nabídky“ a nabízí pouze zobrazení webu Nákupů Google.

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



Funkčnost, obsah a uživatelský dojem

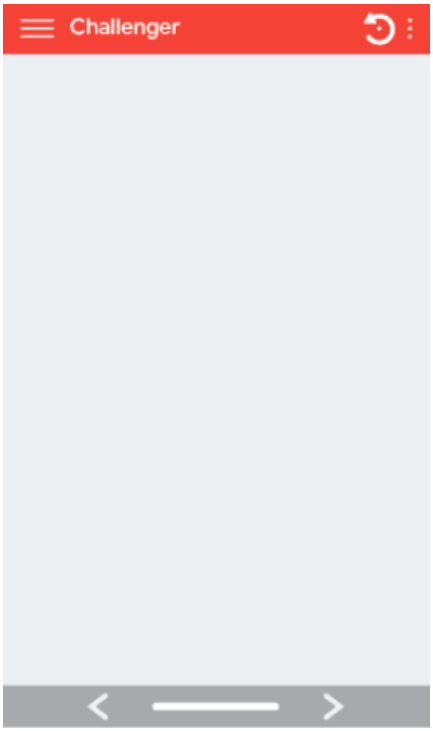
Aplikace musí poskytovat stabilní, responzivní a přitažlivé uživatelské prostředí. Aplikace, které padají, nejsou k ničemu užitečné, nezahrnují žádný zajímavý obsah nebo vykazují jiné chování, které není v souladu s funkčním a přitažlivým uživatelským prostředím, nejsou na Google Play povoleny.

Omezená funkčnost a obsah

Nepovolujeme aplikace, které mají jen omezenou funkčnost a obsah.

Příklad běžného porušení zásad:

- Aplikace, které jsou statické a nezahrnují funkce specifické pro aplikace, například pouze textové aplikace nebo aplikace se soubory PDF
- Aplikace s velmi malým množstvím obsahu, které pro uživatele nejsou ničím zajímavé, například aplikace obsahující jednu tapetu
- Aplikace, které nemají žádný účel ani funkci



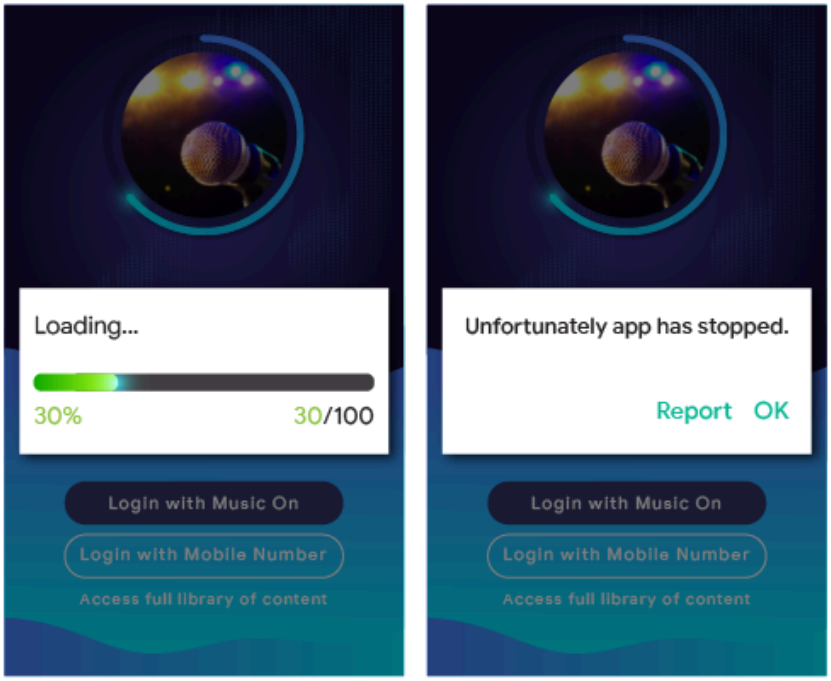
Poruchy funkčnosti

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

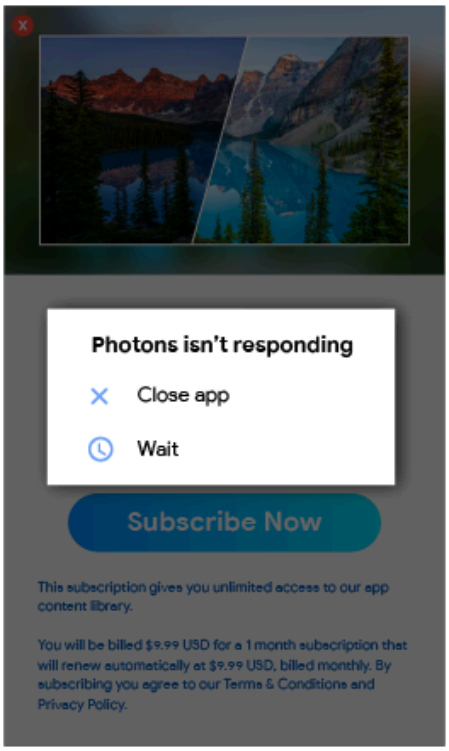
Příklady běžných porušení zásad:

- 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

V případě aplikací, které obsahují funkci přihlášení, musí vývojáři integrovat funkci Smart Lock pro hesla .

Podpora odkazů

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

Technické specifikace

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

Nabízení instalace aplikace

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

- Použít ikonu ke stažení aplikace ve vzhledu Material Design a na instalačním tlačítku použít popisek Instalovat.
- Mít v okamžité aplikaci obsaženy maximálně dvě až tři výzvy k instalaci.
- K prezentování výzvy k instalaci uživatelům nepoužívat banner ani jinou techniku podobnou reklamám.

Další podrobnosti o okamžitých aplikacích a pokyny k uživatelskému rozhraní naleznete v doporučených postupech k uživatelskému prostředí .

Změna stavu zařízení

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

Viditelnost aplikace

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

Identifikátory zařízení

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

- sériové číslo sestavení,
- adresy MAC síťových čipů,
- IMEI, IMSI.

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

Síťový provoz

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

Zásady používání smajlíků v zařízeních Android

Naše zásady ohledně smajlíků jsou určeny k propagaci inkluzivního a konzistentního uživatelského dojmu. Za účelem splnění tohoto cíle musí všechny aplikace pro Android 12 a novější podporovat nejnovější verzi standardu Unicode Emoji .

Aplikace s výchozím standardem Android Emoji bez vlastních implementací už používají nejnovější verzi standardu Unicode Emoji, když jsou spuštěné na Androidu 12 a novějším.

Aplikace s vlastními implementacemi smajlíků (včetně knihoven třetích stran) musí na Androidu 12 a novějším plně podporovat nejnovější verzi Unicode, a to do 4 měsíců od vydání nové verze standardu Unicode Emoji.

Pokyny, jak podporovat moderní smajlíky, najdete v tomto průvodci .

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.

zásady služby Google Play pro 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 právním poradcem 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.

Všechny aplikace, které splňují zásady služby Google Play pro rodiny, se mohou přihlásit k hodnocení pro program Schváleno učiteli. Nemůžeme však zaručit, že aplikace bude do programu Schváleno učiteli zahrnuta.

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.

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

Aktualizace v sekci Cílové publikum a obsah

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

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

Uvedení nepravdivých údajů v Play Console

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

Požadavky zásad pro rodiny

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

1. **Obsah aplikace:** Obsah aplikace přístupný dětem musí být pro děti vhodný. Pokud vaše aplikace zahrnuje obsah, který není celosvětově vhodný, ale je považován za vhodný pro dětské uživatele v určité oblasti, může být aplikace v dané oblasti dostupná (omezený počet oblastí), ale v ostatních oblastech zůstane nedostupná.
2. **Funkce aplikace:** Aplikace nesmí sloužit pouze ke zprostředkovávání zobrazení webových stránek nebo primárně k přesměrovávání uživatele na webové stránky bez svolení vlastníka nebo administrátora příslušných stránek.
3. **Odpovědi v Play Console:** Na otázky ohledně aplikace v Play Console musíte pravdivě odpovídat a aktualizovat je tak, aby přesně reflektovaly veškeré změny aplikace. To zahrnuje mimo jiné i poskytnutí přesných odpovědí o aplikaci v sekcích Cílové publikum a obsah a Zabezpečení údajů a v dotazníku IARC pro hodnocení obsahu.
4. **Způsob nakládání s daty:** 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 ze senzorů mikrofonu a fotoaparátu, údaje o zařízení, Android ID a údaje o využití reklam. Musíte také zajistit, aby se vaše aplikace řídila následujícími způsoby nakládání s daty:
   - Aplikace, které cílí pouze na děti, nesmí přenášet inzertní identifikátor Android (AAID), sériové číslo SIM karty, sériové číslo sestavení, BSSID, MAC, SSID, IMEI ani IMSI.
   - Aplikace, které cílí pouze na děti, při cílení na rozhraní Android API 33 nebo vyšší nesmí vyžadovat oprávnění AD_ID.

- Aplikace, které cílí jak na děti, tak na starší publikum, nesmějí přenášet AAID, sériové číslo SIM karty, sériové číslo sestavení, BSSID, MAC, SSID, IMEI ani IMSI od dětí nebo uživatelů neznámého věku.
- Metody TelephonyManager rozhraní Android API nesmí vyžadovat telefonní číslo zařízení.
- Aplikace, které cílí výhradně na děti, nesmí žádat o přístup k poloze ani shromažďovat, používat a přenášet přesnou polohu.
- Aplikace žádající o přístup k rozhraní Bluetooth musí používat Správce doprovodných zařízení (CDM) (kromě aplikací, které cílí pouze na verze operačního systému zařízení, které se Správcem doprovodných zařízení nejsou kompatibilní).

5. **Rozhraní API a sady SDK:** Musíte zajistit, aby vaše aplikace případná rozhraní API a sady SDK implementovala správně.
   - Aplikace, které cílí výhradně na děti, nesmějí obsahovat žádná rozhraní API ani sady SDK, které nejsou schváleny k použití ve službách určených primárně pro děti.
     - Příkladem může být služba API, která k ověření používá technologii OAuth, jejíž smluvní podmínky uvádějí, že není schválena pro použití ve službách pro děti.
   - Aplikace, které cílí na děti i starší publikum, by neměly implementovat rozhraní API ani sady SDK, které nejsou schváleny k použití ve službách určených pro děti. Mohou je používat pouze za neutrálním věkovým filtrem nebo implementovat způsobem, který nevede ke shromažďování dat od dětí. Aplikace, které cílí na děti i na starší publikum, nesmí vyžadovat přístup k obsahu rozhraní API nebo sady SDK, které nejsou schváleny pro použití ve službách určených pro děti.

6. **Rozšířená realita (RR):** 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 (například Daydream či Oculus).

7. **Sociální aplikace a funkce:** Pokud aplikace umožňují uživatelům sdílení nebo výměnu informací, musíte tyto funkce přesně popsat v dotazníku hodnocení obsahu ve službě Play Console.
   - Sociální aplikace: Jedná se o aplikaci, jejíž hlavní náplní je umožňovat uživatelům sdílení libovolného obsahu nebo komunikaci s širokými skupinami osob. Všechny sociální aplikace, mezi jejichž cílové publikum patří děti, musí dříve, než dětským uživatelům umožní výměnu libovolných médií nebo informací, zobrazit uvnitř aplikace připomenutí o bezpečném chování v online prostředí a rizicích, které online komunikace přináší v reálném světě. Také musíte vyžadovat souhlas dospělé osoby, než dětem bude umožněna výměna osobních údajů.
   - Sociální funkce: Sociální funkce je jakákoli doplňková funkce aplikace, která uživatelům umožňuje sdílet libovolný obsah nebo komunikovat s širokými skupinami osob. Všechny aplikace, mezi jejichž cílové publikum patří děti a mají sociální funkce, musí dříve, než dětským uživatelům umožní výměnu libovolných médií nebo informací, zobrazit uvnitř aplikace připomenutí o bezpečném chování v online prostředí a rizicích, které online komunikace přináší v reálném světě. Také musíte dospělým poskytnout způsob, jak spravovat sociální funkce za dětské uživatele, mimo jiné včetně povolení/zakázání sociální funkce nebo výběru různých úrovní funkce. Před aktivací funkcí, které dětem umožňují výměnu osobních údajů, navíc musíte vyžadovat souhlas dospělé osoby.
   - Souhlas dospělé osoby je nutné získat prostřednictvím mechanismu, který ověří, že uživatel není dítě, a nepovzbuzuje děti k uvedení nepravdivého věku za účelem získání přístupu do sekcí aplikace určených pro dospělé (například PIN, heslo, datum narození dospělého, ověření e-mailu, průkaz totožnosti s fotkou, platební karta nebo rodné číslo).
   - Sociální aplikace, jejichž hlavní náplní je chat s neznámými lidmi, nesmějí cílit na děti. Mezi příklady patří: aplikace pro chat s náhodnými lidmi, seznamovací aplikace, otevřené chatovací místnosti zaměřené na děti apod.

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 odkazující na webové stránky s obsahem, který porušuje programové zásady pro vývojáře Google Play,
- aplikace, které dětem zobrazují reklamy určené pouze dospělým (například násilný obsah, sexuální obsah, obsah týkající se hazardních her).

Reklamy a zpeněžení

Pokud zpeněžujete aplikaci, která ve službě Play cílí na děti, aplikace musí splňovat následující zásady ohledně reklam a zpeněžování obsahu pro rodiny.

Níže uvedené zásady se vztahují na veškeré zpeněžení a reklamy ve vaší aplikaci, včetně reklam, propagace napříč platformami (ve vašich aplikacích i v aplikacích třetích stran), nabídek nákupů v aplikacích nebo jiného komerčního obsahu (například placeného zobrazení produktu). Veškeré zpeněžení a reklamy 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.

Požadavky na reklamy

Pokud se v aplikaci zobrazují reklamy dětem nebo uživatelům neznámého věku, musíte:

- zajistit, aby se reklamy těmto uživatelům zobrazovaly pouze pomocí sad SDK pro reklamy s vlastní certifikací souladu se zásadami služby Google Play pro rodiny,
- 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.

Požadavky na formát reklamy

Zpeněžení a reklamy ve vaší aplikaci nesmí mít klamavý obsah a nesmí být navrženy způsobem, který by měl za následek neúmyslná kliknutí dětských uživatelů.

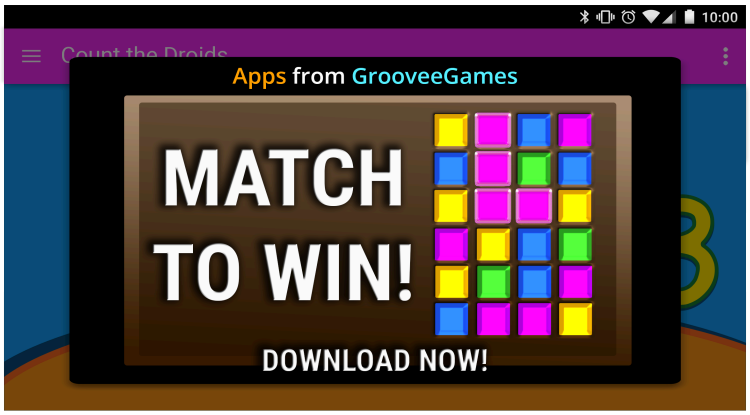
Pokud cílové publikum aplikace zahrnuje pouze děti, jsou následující praktiky zakázány. Pokud cílové publikum aplikace zahrnuje kromě dětí i starší publikum, jsou následující praktiky zakázány při zobrazování reklam dětem nebo uživatelům neznámého věku:

- rušivé zpeněžení a reklamy, včetně případů, kdy zpeněžení nebo reklamy zabírají celou obrazovku nebo narušují běžné používání a neposkytují zřetelnou možnost, jak reklamu zavřít (například reklamní stěny),
- zpeněžení a reklamy, které narušují běžné používání aplikace nebo hry (včetně reklam s nabídkou odměny a reklam, k nimž se uživatelé mohou přihlásit) a které nelze po pěti sekundách zavřít,
- zpeněžení a reklamy, které nenarušují běžné používání aplikace nebo hry se mohou zobrazovat i déle než 5 sekund (např. videoobsah s integrovanými reklamami),
- zpeněžování pomocí vsunutých reklam a inzerce zobrazované ihned po spuštění aplikace,
- umístění více než jedné reklamy na stránku (nepovolujeme například bannerové reklamy, které v jednom umístění zobrazují několik nabídek, nebo zobrazování více než jednoho banneru či videoreklamy),
- zpeněžování a reklamy, které nelze jasně odlišit od obsahu aplikace, jako jsou například zprávy offerwall a některé celostránkové reklamy,
- používání šokujících nebo emocionálně manipulativních taktik s cílem přimět uživatele ke zhlédnutí reklam či k nákupům v aplikaci,
- klamavé reklamy, které uživatele nutí k prokliku tím, že po kliknutí na tlačítko k zavření spouští další reklamu, nebo které se nenadále objevují na místech, kam uživatel obvykle klepá kvůli jiné funkci,
- nerozlišování virtuální herní měny a reálných peněz u nákupů v aplikacích.

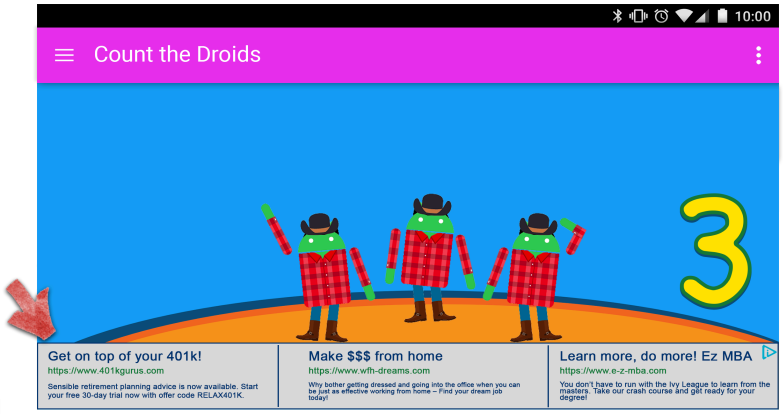
Příklady běžných porušení zásad:

- Zpeněžení a reklamy, které uživateli uhýbají, když se je prstem pokouší zavřít
- Zpeněžení a reklamy, které uživateli nenabízí možnost jejich zavření po pěti (5) sekundách, jak je znázorněno na obrázku níže:

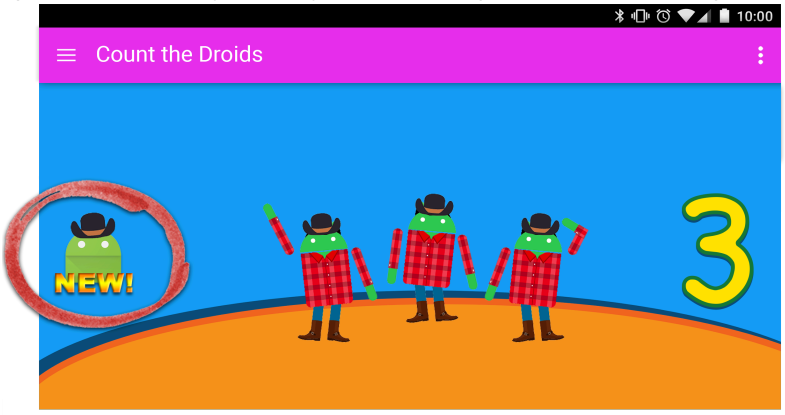
- Zpeněžení a reklamy, které zabírají většinu obrazovky zařízení a neposkytují uživateli jasnou možnost zavření, jako na obrázku níže:



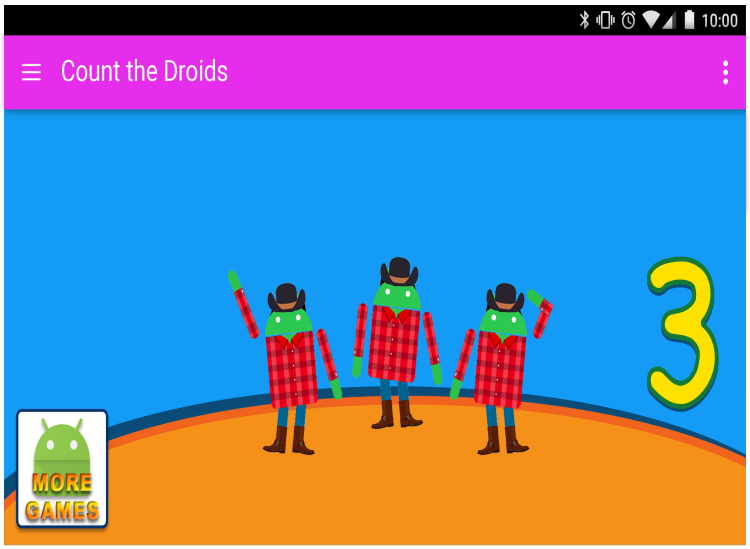
- Bannerové reklamy s několika nabídkami, jako na obrázku níže:



- Zpeněžení a reklamy, které by uživatel mohl považovat za obsah aplikace, jako na obrázku níže:



- Tlačítka, reklamy a další možnosti zpeněžení 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 na jakékoliv jiné škodlivé látky.
- **Hazardní hry**: Reklamy na simulované hazardní hraní, soutěže nebo sázky (včetně bezplatných).
- **Obsah určený pro dospělé a obsah 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 pro dospělé.
- **Násilný obsah**: Reklamy s násilným nebo explicitním obsahem, který není vhodný pro děti.

Sady SDK pro reklamy

Pokud v aplikaci zobrazujete reklamy a vaše cílové publikum zahrnuje pouze děti, musíte používat pouze verze sad SDK pro reklamy s vlastní certifikací pro rodiny . 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 verzí sad SDK pro reklamy s vlastní certifikací pro rodiny.

Další podrobnosti o těchto požadavcích najdete na stránce se zásadami programu sad SDK pro reklamy s vlastní certifikací pro rodiny a aktuální seznam sad SDK pro reklamy s vlastní certifikací pro rodiny najdete zde .

Jestliže používáte službu AdMob, další informace o jejích produktech naleznete v centru nápovědy AdMob .

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

Zásady sad SDK pro reklamy s vlastní certifikací pro rodiny

Google Play se zavázala vytvářet bezpečné prostředí pro děti a rodiny. Klíčovou součástí je zajistit, aby se dětem zobrazovaly pouze reklamy, které jsou přiměřené jejich věku, a aby se s jejich údaji zacházelo náležitým způsobem. S ohledem na tento cíl vyžadujeme, aby sady SDK pro reklamy a platformy pro zprostředkování prostřednictvím vlastní certifikace potvrdily, že jsou vhodné pro děti a splňují

programové zásady služby Google Play pro vývojáře a zásady služby Google Play pro rodiny , včetně požadavků programu sad SDK pro reklamy s vlastní certifikací pro rodiny .

Program sad SDK pro reklamy s vlastní certifikací pro rodiny služby Google Play představuje pro vývojáře důležitý způsob, jak zjistit, které sady SDK pro reklamy nebo platformy pro zprostředkování prostřednictvím vlastní certifikace potvrdily, že jsou vhodné k použití v aplikacích navržených speciálně pro děti.

Nesprávné uvedení jakýchkoliv informací o vaší sadě SDK, včetně informací ve formuláři pro zájemce , může vést k odstranění nebo pozastavení vaší sady SDK z programu sad SDK pro reklamy s vlastní certifikací pro rodiny. Je proto důležité uvádět přesné údaje.

požadavky zásad

Pokud vaši sadu SDK nebo platformu pro zprostředkování využívají aplikace, které jsou součástí programu služby Google Play pro celou rodinu, musíte splnit všechny zásady služby Google Play pro vývojáře, včetně následujících požadavků. Nesplnění kterýchkoliv požadavků zásad může mít za následek odebrání nebo pozastavení v programu sad SDK pro reklamy s vlastní certifikací pro rodiny.

Je vaší odpovědností zajistit, aby vaše sada SDK nebo platforma pro zprostředkování splňovala všechny požadavky. Přečtěte si proto programové zásady služby Google Play pro vývojáře, zásady služby Google Play pro rodiny a požadavky programu sad SDK pro reklamy s vlastní certifikací pro rodiny.

1. **Obsah reklam:** Obsah reklam přístupný dětem musí být pro děti vhodný.
   - Musíte (i) definovat nevhodný obsah a chování reklam a (ii) ve svých smluvních podmínkách nebo zásadách je musíte zakázat. Definice musí splňovat programové zásady služby Google Play pro vývojáře.
   - Musíte také vytvořit metodu hodnocení kreativ 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 pro zájemce poskytuje společnost Google.
   - Musíte zajistit, aby v případě použití nabídek v reálném čase při zobrazování reklam dětem byly kreativy zkontrolovány a splňovaly výše uvedené požadavky.
   - Kromě toho musíte mít mechanismus k vizuální identifikaci kreativ pocházejících z vašeho inventáře (například označení kreativ vodoznakem s logem vaší společnosti nebo podobnou funkci).
2. **Formát reklam:** Musíte zajistit, aby všechny reklamy zobrazované dětským uživatelům splňovaly požadavky na formát reklam pro rodiny, a musíte vývojářům umožnit výběr formátů reklam, které jsou v souladu se zásadami služby Google Play pro rodiny.
   - Reklamy nesmí mít klamavý obsah a nesmí být navrženy způsobem, který by měl za následek neúmyslná kliknutí dětských uživatelů. Jsou zakázány klamavé reklamy, které uživatele nutí k prokliku tím, že po kliknutí na tlačítko k zavření spouští další reklamu, nebo které se nenadále objevují na místech, kam uživatel obvykle klepá kvůli jiné funkci.
   - Jsou zakázány rušivé reklamy, včetně reklam, které zabírají celou obrazovku nebo narušují běžné používání a nenabízejí jasný způsob, jak reklamu zavřít (například reklamní stěny ad wall).
   - Reklamy, které narušují běžné používání aplikace nebo hraní hry, včetně reklam s nabídkou odměny nebo reklam, ke kterým se uživatelé výslovně přihlásili, musí být po 5 sekundách možné zavřít.
   - Není povoleno použití více než jednoho umístění reklamy na stránce. Nejsou například povoleny bannerové reklamy, které zobrazují více nabídek v jednom umístění, a není povoleno zobrazovat více než jeden banner či videoreklamu.
   - Reklamy musí být jasně rozeznatelné od obsahu aplikace. Jsou zakázány zprávy offerwall a reklamy, které by dětští uživatelé nemuseli jasně rozpoznat jako reklamy.

- Reklamy nesmí používat šokující nebo emocionálně manipulativní taktiky s cílem přimět uživatele ke zhlédnutí reklam.

3. **Zájmově orientovaná reklama / remarketing:** Musíte zajistit, aby reklamy zobrazované dětským uživatelům nezahrnovaly zájmově orientovanou reklamu (reklamu cílenou na jednotlivé uživatele, kteří mají určité vlastnosti na základě chování při procházení internetu) nebo remarketing (reklamu zacílenou na jednotlivé uživatele na základě předchozí interakce s aplikací nebo webem).
4. **Způsoby nakládání s daty:** Jako poskytovatel sady SDK musíte být transparentní ohledně toho, jak zacházíte s údaji o uživateli (například s informacemi, které jste o něm a jeho zařízení shromáždili). Musíte uvést, jak vaše sada SDK shromažďuje, používá a sdílí údaje, a tyto údaje smíte používat jen k účelům, které jste uvedli. Tyto požadavky služby Google Play platí nad rámec povinností, které vyplývají z platných právních předpisů na ochranu soukromí a osobních údajů. Musíte uvést shromažďování jakýchkoliv osobních a citlivých údajů od dětí, mimo jiné včetně ověřovacích údajů, dat z mikrofonu a fotoaparátu, údajů o zařízení, Android ID a údajů o využití reklam.
   - Musíte vývojářům umožnit, aby u jednotlivých žádostí nebo aplikací mohli při zobrazování reklam 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 sad SDK pro reklamy určených pro děti byly deaktivovány personalizované reklamy, zájmově orientované reklamy a remarketing.
   - Musíte zajistit, aby při použití nabídek v reálném čase k zobrazování reklam dětem byly indikátory ochrany soukromí předány nabízejícím.
   - Od dětí nebo uživatelů neznámého věku nesmíte přenášet AAID, sériové číslo SIM karty, sériové číslo sestavení, BSSID, MAC, SSID, IMEI ani IMSI.

5. **Platformy pro zprostředkování**: Při zobrazování reklam dětem musíte splnit následující požadavky:
   - Používejte pouze sady SDK pro reklamy s vlastní certifikací pro rodiny 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.

6. **Vlastní certifikace a soulad:** Musíte společnosti Google poskytnout dostatek informací (jako jsou informace uvedené ve formuláři pro zájemce) k ověření, zda sada SDK pro reklamy splňuje zásady a všechny požadavky na vlastní certifikaci. Mimo jiné musíte:
   - poskytnout anglickou jazykovou verzi smluvních podmínek, zásad ochrany soukromí a průvodce integrací pro majitele obsahu své sady SDK nebo platformy pro zprostředkování,
   - odeslat ukázkovou testovací aplikaci, která používá nejnovější kompatibilní verzi sady SDK pro reklamy. Ukázková testovací aplikace musí být plně sestavený a spustitelný balíček APK pro Android, který využívá všechny funkce sady SDK. Požadavky na testovací aplikaci:
     - Musí být odeslána jako úplný spustitelný soubor APK pro Android určený ke spuštění na telefonu.
     - Musí používat nejnovější verzi sady SDK pro reklamy nebo verzi, která bude brzy vydána, která dodržuje zásady služby Google Play.
     - K načítání a zobrazování reklam musí používat všechny funkce sady SDK pro reklamy, včetně volání sady SDK pro reklamy.
     - Musí mít plný přístup ke všem publikovaným/zobrazovaným reklamním plochám v síti, a to prostřednictvím kreativ, které tato testovací aplikace požaduje.
     - Nesmí být omezena geografickou polohou.
     - Pokud je váš inventář určen pro smíšené publikum, testovací aplikace musí umět rozlišovat mezi požadavky na kreativy reklam z celého inventáře, z inventáře vhodného pro děti a z inventáře pro všechny věkové skupiny.
     - Nesmí být omezena na konkrétní reklamy v inventáři, pokud nepoužívá neutrální věkový filtr.

7. Musíte bez větší prodlevy odpovídat na všechny následné žádosti o informace a prostřednictvím vlastní certifikace potvrdit, že všechny nové verze splňují nejnovější programové zásady služby Google Play pro vývojáře, včetně zásad pro rodiny.
8. **Soulad s právními předpisy:** Sady SDK pro reklamy s vlastní certifikací pro rodiny musejí podporovat zobrazování reklam, které je v souladu se všemi relevantními předpisy a nařízeními ohledně dětí, jež se na majitele obsahu mohou vztahovat.
   - Musíte zajistit, aby vaše sada SDK nebo platforma pro zprostředkování byla v souladu se zákonem USA o ochraně soukromí a ochraně dětí na internetu (COPPA) , obecným nařízením EU o ochraně osobních údajů (GDPR) a dalšími příslušnými zákony či předpisy.

     Poznámka: Slovo „děti“ může mít v různých regionech a kontextech různý význam. Je důležité, abyste se svým právním poradcem 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.

Další podrobnosti o požadavcích tohoto programu najdete na stránce Program sad SDK pro reklamy s vlastní certifikací pro rodiny.

Vynucování

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

Rozsah zásad

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

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

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

Nepovolujeme aplikace ani obsah aplikací podrývající 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 systému 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 ochran 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

Při kontrole obsahu a účtů za účelem zjištění, zda jsou nelegální nebo porušují naše zásady, bereme v potaz různé informace, včetně metadat aplikace (např. název a popis), prostředí aplikace, informací o účtu (např. dřívější porušení zásad) a další informace získané z mechanismů nahlašování (pokud jsou k dispozici) a vlastních kontrol.

Pokud vaše aplikace nebo účet vývojáře porušuje některou z našich zásad, podnikneme příslušné níže uvedené kroky. 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 aplikací nebo ve vašem účtu. Vývojáři nesou odpovědnost za vyřešení všech problémů týkajících se porušení zásad. Zároveň se očekává, že věnují zvýšenou pozornost tomu, aby zásadám plně odpovídala i zbývající část aplikace či účtu. Pokud porušení zásad ve svém účtu a všech svých aplikacích nevyřešíte, 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 vašim aplikacím mohou být podniknuta různá donucovací opatření. U aplikací a jejich obsahu kontrolujeme, zda neporušují naše zásady a nejsou škodlivé pro uživatele a celý ekosystém Google Play. Kromě toho, že aplikace kontrolují naši lidé, využíváme také automatické modely. Automatické modely nám pomáhají odhalit více porušení zásad a vyhodnocovat potenciální problémy rychleji, aby služba Google Play byla stále bezpečná pro všechny. Obsah porušující zásady v některých případech odstraňují přímo naše automatické modely. Pokud je potřeba posoudit drobnější nuance (například zohlednit kontext), automatické modely obsah nahlásí našim proškoleným operátorům a analytikům,

kteří ho vyhodnotí. Na základě výsledků těchto manuálních kontrol pak sestavujeme cvičná data k dalšímu zdokonalování našich modelů strojového učení.

Následující sekce popisuje různá opatření, která může služba Google Play podniknout, a jak tato opatření mohou ovlivnit vaši aplikaci nebo účet vývojáře Google Play.

Pokud v oznámení o vynucovacích opatřeních není uvedeno jinak, týkají se všech oblastí. Pozastavená aplikace například nebude k dispozici v žádné oblasti. Pokud není uvedeno jinak, zůstanou tato opatření v platnosti, dokud se proti nim neodvoláte a odvolání nebude schváleno.

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. 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 nenapravíte všechna porušení zásad.

Pozastavení

- Aplikace bude i s případnými předchozími verzemi odstraněna z Google Play a uživatelé ji už nebudou moct 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.
- Soubor APK ani balíček pozastavené aplikace už nelze používat.
- Uživatelé nebudou moci provádět nákupy v aplikaci ani používat funkce fakturace v aplikaci.
- Pozastavení poškozují dobrou pověst vašeho účtu vývojáře Google Play. Větší počet sankcí může vést k ukončení jednotlivých i souvisejících účtů vývojáře Google Play.

Omezená viditelnost

- Objevitelnost 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.
- 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.

Omezení podle oblastí

- Uživatelé si aplikaci mohou stáhnout pouze prostřednictvím Google Play v určených oblastech.
- Uživatelé z jiných oblastí aplikaci v Obchodu Play nenajdou.
- Uživatelé, kteří si aplikaci nainstalovali už dříve, ji mohou v zařízení dál používat, ale nedostanou žádné další aktualizace.
- Omezení podle oblastí nemá vliv na reputaci vašeho účtu vývojáře Google Play.

Stav omezení účtu

- Když je váš účet vývojáře v omezeném stavu, všechny aplikace z vašeho katalogu jsou z Google Play odstraněny, nebudete je moci znovu publikovat a nebudete moci publikovat ani nové aplikace. Přístup do Play Console budete mít i nadále.
- Protože všechny aplikace budou odstraněny, uživatelé neuvidí jejich záznamy v obchodu ani váš profil vývojáře.
- Stávající uživatelé vašich aplikací v nich nebudou moci provádět nákupy v aplikaci ani používat funkce fakturace v aplikaci.
- Play Console budete moci používat i nadále a budete tak týmu Google Play moci poskytnout další informace a opravit informace o svém účtu.
- Až všechna porušení zásad vyřešíte, budete své aplikace moci znovu publikovat.

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 ani váš profil vývojáře.
- Stávající uživatelé nebudou moci provádět nákupy v aplikaci ani ve vašich aplikacích používat funkce fakturace v aplikaci.

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 účtu ukončen.

Spící účty

Spící účty jsou účty vývojářů, které nejsou aktivní nebo byly opuštěny. Spící účty nejsou v dobrém stavu, jak vyžaduje distribuční smlouva pro vývojáře .

Účty vývojářů Google Play jsou určeny pro aktivní vývojáře, kteří publikují nové aplikace a starají se o ty stávající. Abychom zabránili zneužití, spící účty rušíme. Týká se to účtů, které nejsou používány nebo nejsou pravidelně aktivní (nepublikují ani neaktualizují aplikace, nezobrazují si statistiky, nespravují záznamy v obchodu).

Zrušený spící účet bude smazán spolu se všemi přidruženými daty. Registrační poplatek je nevratný. Před zrušením spícího účtu vás budeme informovat. Použijeme k tomu kontaktní údaje daného účtu.

Po zrušení spícího účtu si můžete bez omezení založit nový účet k publikování obsahu na Google Play. Zrušený účet nelze obnovit. Předchozí aplikace ani data nelze zpřístupnit v novém účtu.

Správa a hlášení porušení zásad

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, případně se odvolejte kliknutím sem.

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.

- Ověření aplikací
- 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

Požadavky na Play Console

Aby byla zajištěna bezpečnost našeho živého ekosystému aplikací, Google Play vyžaduje, aby všichni vývojáři splnili požadavky služby Play Console. Tyto požadavky je nutné splnit u všech profilů, které jsou propojeny s vaším účtem vývojáře v Play Console. Ověřené informace se budou zobrazovat na Google Play a budou pomáhat budovat u uživatelů důvěru ve vývojáře. Další informace o tom, jaké údaje se zobrazují na Google Play

Google Play nabízí dva typy vývojářských účtů: osobní účet a účet organizace. Výběr správného typu účtu vývojáře a provedení potřebných ověření je klíčem k hladkému průběhu registrace. Další informace o výběru typu účtu vývojáře

Vývojáři, kteří poskytují následující typy služeb, se při vytváření účtu Play Console musí zaregistrovat jako organizace:

- Finanční produkty a služby, mimo jiné včetně bankovnictví, půjček, obchodování s akciemi, investičních fondů, softwarových peněženek pro kryptoměny a burz kryptoměn. Další informace o zásadách pro finanční služby
- Zdravotní aplikace, jako jsou lékařské aplikace a aplikace pro výzkum na lidských subjektech. Další informace o kategoriích zdravotních aplikací
- Aplikace schválené k používání třídy VpnService . Další informace o zásadách používání služby VPN
- Úřední aplikace, včetně aplikací vyvinutých orgány státní správy nebo jejich jménem.

Po výběru typu účtu musíte splnit následující požadavky:

- Poskytnout přesné informace o účtu vývojáře, včetně následujících podrobností:
  - Celé jméno a adresa
  - Číslo DUNS , pokud se registrujete jako organizace
  - Kontaktní e-mailová adresa a telefonní číslo
  - E-mailová adresa a telefonní číslo vývojáře, které se budou zobrazovat na Google Play (pokud jsou potřeba)
  - Platební metody (pokud jsou potřeba)

- Platební profil Google propojený s vaším účtem vývojáře
- Pokud se registrujete jako organizace, musíte zajistit aktuálnost informací o účtu a příslušné údaje musí být konzistentní s vašimi údaji v profilu Dun & Bradstreet

Před odesláním aplikace musíte:

- Přesně uvést všechny informace a metadata aplikace
- Nahrát zásady ochrany soukromí aplikace a vyplnit požadované informace v sekci Zabezpečení údajů
- Uvést aktivní ukázkový účet, přihlašovací informace a všechny další zdroje potřebné ke kontrole aplikace na Google Play (tzn. přihlašovací údaje, QR kód apod.)

Jako obvykle byste měli zajistit, aby aplikace přinášela stabilní, přitažlivý a responzivní uživatelský dojem, pečlivě zkontrolovat, že veškeré součásti aplikace včetně reklamních sítí, analytických služeb a sad SDK třetích stran splňují programové zásady služby Google Play pro vývojáře, a pokud aplikace cílí na publikum zahrnující děti, musí také splňovat zásady pro rodiny.

Nezapomeňte, že je vaší povinností přečíst si distribuční smlouvu pro vývojáře a všechny programové zásady pro vývojáře a zajistit, aby s nimi aplikace byla v souladu.

Developer Distribution Agreement

Potřebujete další pomoc?

Vyzkoušejte tyto další kroky:

Kontaktujte nás

Řekněte nám víc a my vám pomůžeme