Zasady programu dla deweloperów

(obowiązuje od 9 listopada 2022 roku, o ile nie zaznaczono inaczej)

Wspólnie twórzmy źródło aplikacji i gier, które cieszy się największym zaufaniem na świecie

Twoje innowacje to podstawa naszego wspólnego sukcesu, ale pamiętaj o wynikającej z niego odpowiedzialności. Zasady programu dla deweloperów wraz z Umową dystrybucyjną dla deweloperów są po to, abyśmy razem dalej mogli oferować najbardziej innowacyjne i cieszące się największym zaufaniem aplikacje ponad miliardowi klientów Google Play. Zachęcamy do zapoznania się z naszymi zasadami poniżej.

Treści podlegające ograniczeniom

Użytkownicy na całym świecie codziennie korzystają z Google Play, by uzyskiwać dostęp do aplikacji i gier. Przed przesłaniem aplikacji należy się zastanowić, czy nadaje się ona do udostępnienia w Google Play i czy jest zgodna z przepisami prawa.

Narażanie dzieci na niebezpieczeństwo

Aplikacje, które nie zabraniają użytkownikom tworzenia, przesyłania i rozpowszechniania treści umożliwiających wykorzystywanie dzieci, będą natychmiast usuwane z Google Play. Ta zasada obejmuje też wszystkie materiały związane z wykorzystywaniem seksualnym dzieci. Aby poinformować o treściach w usłudze Google, które mogą przedstawiać wykorzystywanie dziecka, kliknij **Zgłoś nadużycie** . Jeśli znajdziesz tego typu treści w innym miejscu w internecie, skontaktuj się bezpośrednio z odpowiednią organizacją w swoim kraju .

Zabraniamy wykorzystywania aplikacji w celu narażania dzieci na niebezpieczeństwo. Dotyczy to między innymi promowania agresywnych zachowań w stosunku do dzieci, takich jak:

- nieodpowiednie interakcje z dziećmi (np. obmacywanie lub pieszczoty);
- uwodzenie dzieci, np. zaprzyjaźnianie się z dzieckiem w internecie w celu doprowadzenia (online lub offline) do kontaktu seksualnego lub wymiany z dzieckiem zdjęć o charakterze seksualnym;
- seksualizacja osób nieletnich, np. przez prezentowanie zdjęć przedstawiających lub promujących wykorzystywanie seksualne dzieci bądź zachęcających do niego albo zamieszczanie materiałów wizualnych przedstawiających dzieci w sposób, który może skutkować ich wykorzystaniem seksualnym;
- szantaż seksualny (polegający np. na grożeniu dziecku udostępnieniem jego intymnych zdjęć, nawet wtedy, gdy grożący takimi zdjęciami nie dysponuje);
- handel dziećmi, na przykład reklamowanie lub pozyskiwanie dzieci w celu ich wykorzystywania seksualnego.

Jeśli wykryjemy treści zawierające materiały dotyczące wykorzystywania seksualnego dzieci, podejmiemy stosowne działania obejmujące m.in. zawiadomienie organizacji NCMEC (National Center for Missing & Exploited Children). Jeśli uważasz, że dziecko może zostać wykorzystane lub paść ofiarą wykorzystania lub handlu ludźmi albo sądzisz, że doszło już do wymienionych przestępstw, skontaktuj się z lokalnymi organami ścigania oraz organizacją zajmującą się bezpieczeństwem dzieci wskazaną tutaj .

Ponadto niedozwolone są aplikacje przeznaczone dla dzieci, ale zawierające treści o tematyce tylko dla dorosłych, w tym:

- aplikacje obrazujące nadmierną przemoc, krew i okrucieństwo;

- aplikacje przedstawiające szkodliwe bądź niebezpieczne działania lub do nich zachęcające.

Zabraniamy również publikowania aplikacji, które promują negatywne postrzeganie ciała lub siebie, w tym aplikacji przedstawiających w celach rozrywkowych operacje plastyczne, odchudzanie lub inne zabiegi kosmetyczne mające na celu zmianę wyglądu.

Nieodpowiednie treści

Aby zagwarantować, że platforma Google Play jest bezpiecznym i tolerancyjnym miejscem, stworzyliśmy standardy, które definiują i blokują materiały szkodliwe lub nieodpowiednie dla naszych użytkowników.

Treści o charakterze seksualnym i wulgaryzmy

Zabraniamy publikowania aplikacji zawierających lub promujących treści erotyczne i wulgaryzmy, w tym pornografię, oraz wszelkie treści i usługi mające na celu wzbudzenie satysfakcji seksualnej. Zabraniamy publikowania aplikacji i ich treści, które mogą być interpretowane jako promujące akt seksualny w zamian za wynagrodzenie. Treści zawierające nagość mogą być dozwolone, o ile mają charakter edukacyjny, dokumentalny, naukowy lub artystyczny i nie są użyte w sposób nieuzasadniony.

Jeśli aplikacja zawiera treści, które naruszają te zasady, ale są uznawane za odpowiednie w konkretnym regionie, może ona być dostępna dla użytkowników w tym regionie, ale nie będzie dostępna w innych regionach.

Aby zagwarantować, że platforma Google Play jest bezpiecznym i tolerancyjnym miejscem, stworzyliśmy standardy, które definiują i blokują materiały szkodliwe lub nieodpowiednie dla naszych użytkowników.

- przedstawianie nagości w kontekście erotycznym lub póz o charakterze jednoznacznie seksualnym, jeśli osoba jest w pełni naga, ma zamazane miejsca intymne lub jest tylko nieznacznie okryta ubraniem w sposób, który byłby nie do przyjęcia w miejscu publicznym;
- przedstawianie, również za pomocą animacji i ilustracji, aktów seksualnych lub póz o charakterze jednoznacznie seksualnym bądź przedstawianie części ciała w kontekście seksualnym;
- treści przedstawiające lub stanowiące gadżety bądź poradniki erotyczne oraz ukazujące nielegalne czynności seksualne i fetysze;
- treści lubieżne lub wulgarne – w tym między innymi wulgaryzmy, obelgi, przekleństwa oraz słowa kluczowe nawiązujące do treści dla dorosłych / treści erotycznych zamieszczone w informacjach o aplikacji lub w samej aplikacji;
- treści przedstawiające, opisujące lub promujące zoofilię;
- aplikacje promujące rozrywkę związaną z seksem, usługi towarzyskie lub inne usługi, które mogą zostać zinterpretowane jako świadczenie usług seksualnych za pieniądze, w tym między innymi sponsoring lub układy seksualne, w których jedna z osób oczekuje lub sugeruje, że druga będzie przekazywać jej pieniądze, prezenty lub zapewniać pomoc finansową (tzw. sugardating);
- aplikacje poniżające lub uprzedmiotawiające inne osoby, np. aplikacje, które oferują rzekomo możliwość rozbierania innych, nawet jeśli opisuje się je jako aplikacje żartobliwe lub rozrywkowe.

Szerzenie nienawiści

Zabraniamy publikowania aplikacji promujących przemoc lub szerzących nienawiść do poszczególnych osób lub grup osób z powodu ich pochodzenia rasowego lub etnicznego, wyznania, niepełnosprawności, wieku, narodowości, statusu weterana, orientacji seksualnej, płci, tożsamości płciowej, kasty, statusu imigranta lub innego aspektu wiążącego się z systemową dyskryminacją lub marginalizacją.

W niektórych krajach zgodnie z lokalnymi przepisami i regulacjami prawnymi możemy blokować aplikacje zawierające treści edukacyjne, dokumentalne, naukowe lub artystyczne dotyczące nazizmu.

Aby zagwarantować, że platforma Google Play jest bezpiecznym i tolerancyjnym miejscem, stworzyliśmy standardy, które definiują i blokują materiały szkodliwe lub nieodpowiednie dla naszych użytkowników.

- treści lub wypowiedzi mające na celu udowodnienie, że chroniona grupa osób jest nieludzka, gorsza lub zasługuje na nienawiść;
- aplikacje zawierające nienawistne wypowiedzi, obelgi, stereotypy lub teorie na temat chronionej grupy osób, przedstawiające te osoby jako wyróżniające się negatywnymi cechami (np. złymi intencjami, zepsuciem czy nikczemnością) albo w sposób bezpośredni lub pośredni mówiące o tym, że dana grupa osób stanowi zagrożenie;
- treści lub wypowiedzi nakłaniające do nienawiści bądź dyskryminacji grupy osób tylko dlatego, że należą one do grupy chronionej;
- treści promujące symbolikę kojarzoną z nienawiścią, np. flagi, symbole, insygnia lub inne przedmioty albo zachowania związane z grupami szerzącymi nienawiść.

Przemoc

Zabraniamy publikowania aplikacji przedstawiających nieuzasadnioną przemoc lub inne niebezpieczne czynności oraz umożliwiających ich wykonanie. Generalnie dopuszczamy aplikacje przedstawiające fikcyjną przemoc w kontekście gry, np. w formie kreskówki, a także treści dotyczące polowań i wędkarstwa.

Aby zagwarantować, że platforma Google Play jest bezpiecznym i tolerancyjnym miejscem, stworzyliśmy standardy, które definiują i blokują materiały szkodliwe lub nieodpowiednie dla naszych użytkowników.

- Drastyczne przedstawianie lub realistyczne opisy przemocy albo gróźb brutalnej przemocy względem ludzi bądź zwierząt
- Aplikacje promujące samookaleczanie się, samobójstwo, zaburzenia odżywiania, zabawy w duszenie lub inne czynności, które mogą spowodować poważne obrażenia lub śmierć.

Treści związane z terroryzmem

Nie zezwalamy organizacjom terrorystycznym na publikowanie aplikacji w Google Play w żadnym celu, w tym do prowadzenia rekrutacji.

Zabronione jest publikowanie aplikacji związanych z terroryzmem, na przykład zawierających treści promujące akty terroru, podżegające do przemocy czy pochwalające ataki terrorystyczne. Jeśli treści związane z terroryzmem są publikowane w celach edukacyjnych, dokumentalnych, naukowych lub artystycznych, należy podać odpowiednie informacje, które pomogą użytkownikom zrozumieć ich kontekst.

Niebezpieczne organizacje i ruchy społeczne

Zabronione jest publikowanie aplikacji w Google Play przez ruchy społeczne i organizacje, które brały udział, przygotowują się lub przyznały się do aktów przemocy przeciwko ludności cywilnej – w dowolnych celach (w tym rekrutacji).

Zabronione jest publikowanie aplikacji z treściami związanymi z planowaniem, przygotowywaniem i gloryfikowaniem aktów przemocy przeciwko ludności cywilnej. Jeśli aplikacja zawiera takie treści publikowane w celach edukacyjnych, dokumentalnych, naukowych lub artystycznych, należy podać odpowiednie informacje, które pomogą użytkownikom zrozumieć ich kontekst.

Dramatyczne wydarzenia

Zabraniamy publikowania aplikacji, które nie wykazują odpowiedniej wrażliwości w odniesieniu do ważnych wydarzeń społecznych, kulturalnych lub politycznych, takich jak zagrożenia dla ludności cywilnej, klęski żywiołowe, zagrożenia dla zdrowia publicznego, konflikty, śmierć lub inne tragiczne

sytuacje, bądź czerpią z takich wydarzeń korzyści. Aplikacje zawierające treści związane z dramatycznymi wydarzeniami są zwykle dozwolone, jeśli są to materiały edukacyjne, dokumentalne, naukowe lub artystyczne albo mają na celu ostrzeżenie użytkowników przed dramatycznym wydarzeniem lub poinformowanie ich o nim.

Aby zagwarantować, że platforma Google Play jest bezpiecznym i tolerancyjnym miejscem, stworzyliśmy standardy, które definiują i blokują materiały szkodliwe lub nieodpowiednie dla naszych użytkowników.

- brak wrażliwości w obliczu śmierci jakiejś osoby bądź grupy osób na skutek samobójstwa, przedawkowania, choroby itp.;
- zaprzeczanie wystąpieniu poważnego tragicznego wydarzenia, które zostało dobrze udokumentowane;
- prawdopodobne czerpanie korzyści ze zdarzenia o charakterze wrażliwym bez wyraźnej korzyści dla jego ofiar;
- aplikacje naruszające wytyczne przedstawione w artykule Wymagania dotyczące aplikacji związanych z chorobą koronawirusową 2019 (COVID-19) .

Dokuczanie i nękanie

Zabronione jest publikowanie aplikacji zawierających groźby, nękanie lub dokuczanie bądź umożliwiających wykonanie takich działań.

Aby zagwarantować, że platforma Google Play jest bezpiecznym i tolerancyjnym miejscem, stworzyliśmy standardy, które definiują i blokują materiały szkodliwe lub nieodpowiednie dla naszych użytkowników.

- Dręczenie ofiar konfliktów międzynarodowych i religijnych.
- treści, które mają służyć do wykorzystywania innych osób – wyłudzanie, szantaż itp.;
- udostępnianie treści w celu publicznego upokorzenia innej osoby;
- Nękanie ofiar tragicznych wydarzeń bądź ich przyjaciół i rodzin.

Produkty niebezpieczne

Zabronione jest publikowanie aplikacji służących do sprzedawania materiałów wybuchowych, broni palnej, amunicji lub niektórych akcesoriów do broni palnej.

- Objęte zakazem są akcesoria, które umożliwiają symulowanie ognia ciągłego lub przerobienie broni pozwalające prowadzić ogień ciągły (np. kolby typu „bump”, spusty typu „gatling”, automatyczne zaczepy spustowe, zestawy części do przerabiania), oraz magazynki i taśmy nabojowe na ponad 30 nabojów.

Zabronione jest publikowanie aplikacji dostarczających instrukcje na temat wytwarzania materiałów wybuchowych, broni palnej, amunicji, akcesoriów do broni palnej, do których dostęp jest ograniczony, lub innych rodzajów broni. Obejmuje to instrukcje przerabiania broni palnej w celu uzyskania możliwości prowadzenia ognia ciągłego lub symulacji ognia ciągłego.

Marihuana

Zabronione jest publikowanie aplikacji ułatwiających sprzedaż marihuany i produktów z marihuaną (niezależnie od ich legalności).

Aby zagwarantować, że platforma Google Play jest bezpiecznym i tolerancyjnym miejscem, stworzyliśmy standardy, które definiują i blokują materiały szkodliwe lub nieodpowiednie dla naszych użytkowników.

- umożliwianie użytkownikom zamawiania marihuany z użyciem funkcji koszyka w aplikacji;
- pomaganie użytkownikom w organizowaniu dostawy lub odbioru marihuany;

- ułatwianie sprzedaży produktów z THC (tetrahydrokannabinolem), w tym produktów takich jak oleje konopne zawierające THC.

Tytoń i alkohol

Zabraniamy publikowania aplikacji ułatwiających sprzedaż tytoniu (w tym e-papierosów i waporyzatorów do tytoniu) oraz zachęcających do nielegalnego lub niewłaściwego używania alkoholu bądź tytoniu.

Aby zagwarantować, że platforma Google Play jest bezpiecznym i tolerancyjnym miejscem, stworzyliśmy standardy, które definiują i blokują materiały szkodliwe lub nieodpowiednie dla naszych użytkowników.

- Przedstawianie albo zachęcanie do spożywania alkoholu lub używania tytoniu przez osoby nieletnie albo do sprzedaży takich produktów nieletnim.
- sugerowanie, że używanie tytoniu może poprawić status społeczny, życie seksualne bądź zawodowe, intelekt lub kondycję fizyczną;
- przedstawianie nadmiernego spożywania alkoholu w sposób korzystny, m.in. przedstawianie w pozytywnym świetle spożywania dużych ilości alkoholu, upijania się i zawodów w piciu.

Usługi finansowe

Zabronione jest publikowanie aplikacji, które oferują użytkownikom szkodliwe lub wprowadzające w błąd produkty i usługi finansowe.

Na potrzeby tych zasad za produkty i usługi finansowe uznaje się produkty i usługi związane z zarządzaniem pieniędzmi i kryptowalutami lub ich inwestowaniem (w tym spersonalizowane doradztwo).

Jeśli aplikacja zawiera lub promuje produkty i usługi finansowe, musi być zgodna ze wszystkimi przepisami obowiązującymi w krajach i regionach, w których ma być dostępna. Na przykład musi zawierać określone informacje wymagane przez lokalne przepisy.

Opcje binarne

Zabronione jest publikowanie aplikacji, które umożliwiają użytkownikom handel opcjami binarnymi.

Kryptowaluty

Zabronione jest publikowanie aplikacji, które kopią kryptowaluty na urządzeniach. Dozwolone są aplikacje do zdalnego zarządzania kopaniem kryptowalut.

Kredyty konsumpcyjne

Kredyt konsumpcyjny to jednorazowe pożyczenie pieniędzy indywidualnemu konsumentowi przez osobę fizyczną, organizację bądź inny podmiot w celu innym niż sfinansowanie zakupu środka trwałego lub edukacji. Aby móc podjąć świadomą decyzję o zaciągnięciu kredytu konsumpcyjnego, konsumenci potrzebują informacji o jakości, warunkach, opłatach, harmonogramie spłaty, ryzyku i korzyściach związanych z produktami kredytowymi.

- Przykłady: kredyty konsumpcyjne, chwilówki, pożyczki społecznościowe, pożyczki pod zastaw.
- Przykłady nieobjęte tą definicją: kredyty hipoteczne, kredyty samochodowe, odnawialne linie kredytowe (np. karty kredytowe, osobiste linie kredytowe).

Aplikacje, które oferują kredyty konsumpcyjne, w tym aplikacje, które bezpośrednio oferują kredyty, służą do zdobywania potencjalnych klientów lub łączą klientów z zewnętrznymi pożyczkodawcami, muszą mieć w Konsoli Play kategorię „Finanse” oraz zawierać w metadanych te informacje:

- minimalny i maksymalny okres spłaty;
- maksymalną rzeczywistą roczną stopę oprocentowania (RRSO), która zwykle obejmuje odsetki, opłaty i inne roczne koszty, lub podobną stopę oprocentowania obliczoną zgodnie z lokalnymi przepisami prawa;
- modelowy przykład całkowitego kosztu kredytu wraz z kwotą kapitału i wszystkimi obowiązującymi opłatami;
- politykę prywatności zawierającą szczegółowy opis sposobów odczytywania, zbierania, wykorzystywania oraz udostępniania danych osobowych i informacji poufnych użytkownika.

Nie zezwalamy na aplikacje, które promują kredyty konsumpcyjne wymagające spłaty w całości w ciągu maksymalnie 60 dni od daty udzielenia (nazywamy je „krótkoterminowymi kredytami konsumpcyjnymi").

Kredyty konsumpcyjne z wysokim RRSO

W Stanach Zjednoczonych nie zezwalamy na aplikacje oferujące kredyty konsumpcyjne o rzeczywistej rocznej stopie oprocentowania (RRSO) wynoszącej 36% lub więcej. Aplikacje do kredytów konsumpcyjnych w USA muszą wyświetlać maksymalne RRSO obliczone zgodnie z ustawą TILA (Truth in Lending Act) .

Te zasady dotyczą aplikacji bezpośrednio oferujących kredyty lub służących do zdobywania potencjalnych klientów oraz tych, które łączą konsumentów z zewnętrznymi pożyczkodawcami.

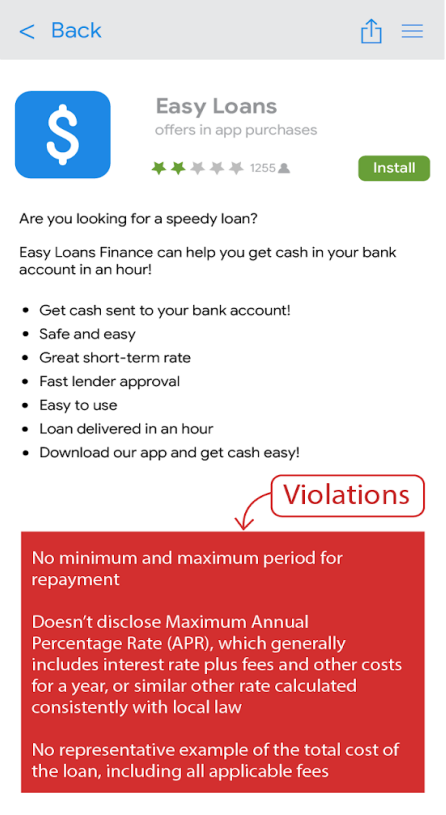
Dodatkowe wymagania dotyczące aplikacji do kredytów konsumpcyjnych obowiązujące na Filipinach oraz w Indiach i Indonezji.

Aplikacje do kredytów konsumpcyjnych na Filipinach oraz w Indiach i Indonezji muszą dodatkowo spełniać wymagania określone poniżej.

1. **Indie**
   - Musisz wypełnić Deklarację dotyczącą aplikacji do kredytów konsumpcyjnych w Indiach i przedstawić wymagane dokumenty. Przykład:
     - Jeśli masz licencję Reserve Bank of India (RBI) na udzielanie kredytów konsumpcyjnych, musisz przedstawić nam jej kopię.
     - Jeśli nie zajmujesz się bezpośrednio udzielaniem kredytów, a jedynie udostępniasz platformę, na której zarejestrowane niebankowe instytucje finansowe lub banki świadczą takie usługi użytkownikom, musisz dokładnie zaznaczyć to w swojej deklaracji.
       - Dodatkowo nazwy wszystkich zarejestrowanych niebankowych instytucji finansowych i banków muszą być dobrze widoczne dla użytkowników w opisie aplikacji.
   - Pamiętaj o tym, aby nazwa konta dewelopera odpowiadała nazwie powiązanej, zarejestrowanej firmy podanej w deklaracji.
2. **Indonezja**
   - Musisz wypełnić Deklarację dotyczącą aplikacji do kredytów konsumpcyjnych w Indonezji i przedstawić wymagane dokumenty. Przykład:
     - Jeśli Twoja aplikacja jest zaangażowana w działanie usług pożyczkowych opartych na technologii informatycznej zgodnie z rozporządzeniem OJK nr 77/POJK.01/2016 (które od czasu do czasu może być aktualizowane), musisz przesłać do weryfikacji kopię ważnej licencji.
   - Pamiętaj o tym, aby nazwa konta dewelopera odpowiadała nazwie powiązanej, zarejestrowanej firmy podanej w deklaracji.
3. **Filipiny**
   - Musisz wypełnić Deklarację dotyczącą aplikacji do kredytów konsumpcyjnych na Filipinach i przedstawić wymagane dokumenty.
     - Wszystkie organizacje finansowe i udzielające pożyczek z wykorzystaniem platform pożyczkowych online muszą uzyskać numer rejestracyjny SEC i numer certyfikatu urzędowego (CA) od filipińskiej Komisji ds. Papierów Wartościowych i Giełd (PSEC).

- Dodatkowo musisz podać w opisie aplikacji nazwę korporacji, nazwę firmy, numer rejestracyjny PSEC i certyfikat urzędowy na prowadzenie organizacji finansowej lub pożyczkowej.
- Aplikacje związane z działaniami crowdfundingowymi opartymi na pożyczkach, takimi jak pożyczki peer-to-peer (P2P) lub działania zdefiniowane w przepisach dotyczących crowdfundingu, muszą przetwarzać transakcje z udziałem pośredników crowdfundingowych zarejestrowanych w PSEC.

Aby zagwarantować, że platforma Google Play jest bezpiecznym i tolerancyjnym miejscem, stworzyliśmy standardy, które definiują i blokują materiały szkodliwe lub nieodpowiednie dla naszych użytkowników.



Hazard

Dopuszczamy aplikacje umożliwiające hazard na pieniądze, reklamy promujące taki hazard, programy lojalnościowe z grywalizacją oraz gry typu daily fantasy sports, które spełniają określone wymagania.

Aplikacje hazardowe

Z uwzględnieniem ograniczeń i wymogów wszystkich zasad Google Play, akceptujemy aplikacje, które umożliwiają lub ułatwiają uprawianie hazardu online w wybranych krajach, o ile deweloper ukończy proces zgłoszenia aplikacji hazardowych udostępnianych w Google Play, jest zatwierdzonym operatorem państwowym lub jest zarejestrowany jako licencjonowany operator w odpowiedniej państwowej instytucji ds. gier hazardowych w danym kraju i przedstawia ważną licencję na prowadzenie działalności związanej z rodzajem usługi hazardowej online, którą chce oferować w danym kraju.

Akceptujemy tylko licencjonowane lub autoryzowane aplikacje hazardowe, które zawierają te rodzaje usług hazardowych online:

- gry hazardowe online;
- zakłady sportowe;

- wyścigi konne (w miejscach, gdzie licencja jest wymagana niezależnie od licencji na zakłady sportowe);
- loterie;
- gry typu daily fantasy sports.

Uprawnione aplikacje muszą spełniać te wymagania:

- Deweloper musi ukończyć proces zgłoszenia aplikacji, aby móc udostępnić ją w Google Play.
- Aplikacja musi być zgodna ze wszystkimi przepisami i standardami branżowymi obowiązującymi w kraju, w którym jest udostępniana.
- Deweloper musi mieć ważną licencję na prowadzenie działalności hazardowej w każdym kraju lub stanie/regionie, w którym udostępnia aplikację.
- Deweloper nie może oferować rodzaju produktu hazardowego, który jest poza zakresem jego licencji na prowadzenie działalności hazardowej.
- Aplikacja musi uniemożliwiać użytkownikom niepełnoletnim korzystanie z niej.
- Aplikacja musi uniemożliwiać dostęp do niej i korzystanie z niej w krajach, stanach/regionach lub obszarach geograficznych, w których nie obowiązuje licencja dewelopera na prowadzenie działalności hazardowej.
- Aplikacja NIE może być oferowana jako płatna w Google Play ani używać Rozliczeń w aplikacji przez Google Play.
- Aplikacja musi być dostępna do pobrania i zainstalowania bezpłatnie ze Sklepu Google Play.
- Aplikacja musi mieć ocenę AO (tylko dla dorosłych) lub odpowiednik w klasyfikacji IARC.
- Aplikacja i jej opis w sklepie muszą w czytelny sposób przedstawiać informacje o odpowiedzialnym hazardzie.

Inne aplikacje oferujące gry, konkursy i zawody na pieniądze

W przypadku pozostałych aplikacji, które nie spełniają powyższych wymagań dotyczących aplikacji hazardowych i które nie są uwzględnione w poniższej sekcji „Wdrożenia pilotażowe w innych grach na pieniądze”, nie zezwalamy na publikowanie treści ani usług umożliwiających lub ułatwiających zawieranie zakładów, obstawianie stawek lub uczestniczenie w grach bądź konkursach na pieniądze (dotyczy to także zakupów w aplikacji za pieniądze) w celu uzyskania nagrody pieniężnej. Chodzi tu m.in. o kasyna online, zakłady sportowe, loterie oraz gry, które akceptują pieniądze i oferują możliwość wygrania nagrody materialnej lub pieniężnej (z wyjątkiem dopuszczonych programów lojalnościowych z grywalizacją spełniających poniższe wymogi).

Przykłady naruszenia zasad:

- gry, które akceptują pieniądze w zamian za możliwość wygrania nagrody materialnej lub pieniężnej;
- aplikacje z elementami lub funkcjami nawigacyjnymi (np. pozycjami menu, kartami, przyciskami, komponentami WebView itp.) zawierającymi „wezwanie do działania”, takiego jak zawarcie zakładu, obstawienie stawek lub wzięcie udziału w grach, konkursach lub zawodach na pieniądze (na przykład aplikacje, które zachęcają użytkowników do obstawiania zakładu, zarejestrowania się lub wzięcia udziału w grze w zamian za szansę wygrania nagrody pieniężnej);
- aplikacje, które akceptują lub kontrolują zakłady, waluty w aplikacji, wygrane albo wpłaty w celach hazardowych lub w celu uzyskania nagrody materialnej bądź pieniężnej.

Wdrożenia pilotażowe w innych grach na pieniądze

W wybranych krajach możemy od czasu do czasu organizować programy pilotażowe związane z pewnymi rodzajami gier na pieniądze. Szczegółowe informacje znajdziesz na tej stronie w Centrum pomocy .

Programy lojalnościowe z grywalizacją

Tam, gdzie jest to dozwolone przez prawo i nie podlega dodatkowym wymogom związanym z hazardem lub licencjami na gry, zezwalamy na programy lojalnościowe, w ramach których użytkownicy otrzymują nagrody materialne lub ekwiwalent pieniężny, zgodnie z tymi wymaganiami Sklepu Play:

Wymagania dotyczące wszystkich aplikacji (gier i pozostałych):

- Korzyści, bonusy i nagrody wynikające z programu lojalnościowego muszą mieć wyraźny charakter uzupełniający lub być uzależnione od kwalifikującej się transakcji pieniężnej w aplikacji (gdzie kwalifikująca się transakcja pieniężna musi być oddzielną, autentyczną transakcją w celu dostarczenia towarów lub usług niezależnie od programu lojalnościowego) i nie mogą podlegać zakupowi ani żadnemu rodzajowi wymiany. W przeciwnym razie wspomniane korzyści, bonusy i nagrody są niezgodne z Zasadami dotyczącymi gier, konkursów i hazardu na pieniądze.
  - Na przykład żadna część kwalifikującej się transakcji pieniężnej nie może stanowić opłaty ani zakładu za udział w programie lojalnościowym, a kwalifikująca się transakcja pieniężna nie może skutkować zakupem towarów lub usług powyżej ich standardowej ceny.

Aplikacje, które są grami :

- Punkty lojalnościowe i nagrody obejmujące korzyści, bonusy lub nagrody powiązane z kwalifikującą się transakcją pieniężną mogą być przyznawane i wykorzystywane tylko na podstawie stałego wskaźnika, który jest wyraźnie udokumentowany w aplikacji oraz w powszechnie dostępnych zasadach programu. Dodatkowo uzyskane korzyści lub wartości do wykorzystania **nie** mogą stanowić zakładu, nagrody ani być spotęgowane przez statystyki gracza lub wyniki oparte na losowości.

Aplikacje inne niż gry:

- Punkty lojalnościowe i nagrody mogą być powiązane z konkursem lub wynikami opartymi na losowości, jeśli spełniają poniższe wymagania. Programy lojalnościowe, w których można odnosić korzyści albo otrzymywać bonusy lub nagrody w wyniku kwalifikującej się transakcji pieniężnej, muszą:
  - mieć opublikowane oficjalne zasady programu w aplikacji;
  - w przypadku programów z systemami przyznawania nagród opartymi na losowości lub zmiennych – w oficjalnych warunkach programu muszą zawierać informacje na temat 1) prawdopodobieństwa uzyskania konkretnej wygranej (w programach korzystających ze stałego prawdopodobieństwa) oraz 2) metody selekcji, np. jakie zmienne decydują o wygranej (w pozostałych programach tego typu);
  - określać stałą liczbę zwycięzców, stały termin przyjmowania zgłoszeń i datę przyznania nagrody w przypadku każdej promocji, zgodnie z oficjalnymi warunkami programu obejmującego losowania, loterie lub inne podobne rodzaje promocji;
  - zawierać w oficjalnych warunkach programu oraz w widocznym miejscu w aplikacji wszelkie informacje o stałym tempie gromadzenia i wykorzystywania punktów lojalnościowych lub nagród.

Typ aplikacji z programem lojalnościowym	Programy lojalnościowe z grywalizacją i nagrody zmienne	Nagrody w programach lojalnościowych oparte na stałym wskaźniku/harmonogramie	Konieczność określenia warunków programu lojalnościowego	Konieczność określenia w warunkach prawdopodobieństw wygranej lub metod selekcji w programi lojalnościowym opartym na losowości

Typ aplikacji z programem lojalnościowym	Programy lojalnościowe z grywalizacją i nagrody zmienne	Nagrody w programach lojalnościowych oparte na stałym wskaźniku/harmonogramie	Konieczność określenia warunków programu lojalnościowego	Konieczność określenia w warunkach prawdopodobieństw wygranej lub metod selekcji w programi lojalnościowym opartym na losowości
Gra	Niedozwolone	Dozwolone	Wymagane	Nie dotyczy (aplikacj będące grami nie mogą mieć elementó opartych na losowoś w programie lojalnościowym)
Aplikacja niebędąca grą	Dozwolone	Dozwolone	Wymagane	Wymagane

Reklamy hazardu oraz gier, konkursów i zawodów na prawdziwe pieniądze w aplikacjach udostępnianych w Google Play

Dozwolone są aplikacje reklamujące hazard, gry, konkursy i zawody na pieniądze, jeśli spełniają one te wymagania:

- Aplikacja i reklama (od reklamodawcy) muszą być zgodne ze wszystkimi przepisami i standardami branżowymi obowiązującymi w miejscu wyświetlania reklamy.
- Reklama musi spełniać wszystkie obowiązujące lokalne wymagania dotyczące licencji w odniesieniu do wszystkich promowanych produktów i usług związanych z hazardem.
- Aplikacja nie może wyświetlać reklam związanych z hazardem osobom, które nie ukończyły 18 lat.
- Aplikacja nie może należeć do programu Dla całej rodziny.
- Aplikacja nie może być kierowana do osób w wieku poniżej 18 lat.
- W przypadku reklamowania aplikacji hazardowej (zgodnie z definicją powyżej) strona docelowa reklamy, strona z informacjami o reklamowanej aplikacji lub sama aplikacja musi zawierać wyraźne informacje o odpowiedzialnym hazardzie.
- Aplikacja nie może zawierać treści symulujących hazard (jak np. aplikacje typu social casino lub aplikacje z wirtualnymi automatami do gier).
- Aplikacja nie może zawierać funkcji pomocnych w grach hazardowych, grach, loteriach lub zawodach na pieniądze ani też funkcji towarzyszących (np. pomocnych w zawieraniu zakładów, realizowaniu wypłat, śledzeniu wyników i osiągów sportowych, szacowaniu prawdopodobieństwa różnych wyników czy zarządzaniu środkami przeznaczonymi na hazard).
- Zawartość aplikacji nie może promować usług związanych z grami hazardowymi, grami, loteriami czy zawodami na pieniądze ani też kierować użytkowników do takich usług.

Reklamy dotyczące hazardu, gier, loterii lub zawodów na pieniądze mogą być wyświetlane tylko w aplikacjach, które spełniają wszystkie wspomniane warunki (powyżej).Dozwolone aplikacje hazardowe (zgodnie z definicją powyżej) i dozwolone gry typu daily fantasy sports (zgodnie z definicją poniżej) spełniające wymagania z punktów 1–6 powyżej mogą zawierać reklamy dotyczące hazardu, gier, loterii lub zawodów na pieniądze.

Przykłady naruszenia zasad:

- aplikacja przeznaczona dla osób niepełnoletnich wyświetlająca reklamę usług hazardowych;
- gra symulująca kasyno, która promuje prawdziwe kasyna lub kieruje użytkowników do prawdziwych kasyn;

- specjalna aplikacja do śledzenia prawdopodobieństwa wystąpienia różnych wyników sportowych, zawierająca zintegrowane reklamy hazardu prowadzące do witryny oferującej zakłady sportowe;
- aplikacje, które zawierają reklamy hazardu naruszające nasze zasady dotyczące reklam wprowadzających w błąd, np. reklamy wyświetlane użytkownikom jako przyciski, ikony lub inne interaktywne elementy w aplikacji.

Aplikacje typu fantasy sports

Dozwolone są wyłącznie aplikacje typu fantasy sports (zgodnie z definicją określoną przez obowiązujące przepisy lokalne), które spełniają te wymagania:

- Aplikacja jest: 1) rozpowszechniana tylko w Stanach Zjednoczonych lub 2) zgodna z wymaganiami dotyczącymi aplikacji hazardowych i procedurą zgłoszeniową dla krajów poza Stanami Zjednoczonymi, zgodnie z opisem powyżej.
- Deweloper musi przesłać aplikację DFS do weryfikacji . Po zatwierdzeniu będzie ją można udostępnić w Google Play.
- Aplikacja musi być zgodna ze wszystkimi przepisami i standardami branżowymi obowiązującymi w krajach, w których jest udostępniana.
- Aplikacja musi uniemożliwiać użytkownikom niepełnoletnim robienie zakładów lub przeprowadzanie transakcji pieniężnych w aplikacji.
- Aplikacja NIE może być oferowana jako płatna w Google Play, a także NIE może używać Rozliczeń w aplikacji przez Google Play.
- Aplikacja musi być dostępna do pobrania i zainstalowania bezpłatnie ze Sklepu.
- Aplikacja musi mieć ocenę AO (tylko dla dorosłych) lub odpowiednik według klasyfikacji IARC.
- Aplikacja i jej opis w Sklepie Play muszą w czytelny sposób przedstawiać informacje o odpowiedzialnym hazardzie.
- Aplikacja musi być zgodna ze wszystkimi przepisami i standardami branżowymi obowiązującymi w USA lub na terytorium USA, w którym jest udostępniana.
- Deweloper musi mieć ważną licencję w każdym stanie i na każdym terytorium USA, które wymagają licencji na rozpowszechnianie aplikacji typu fantasy sports.
- Aplikacja musi uniemożliwiać używanie jej w stanach i na terytoriach USA, na terenie których deweloper nie ma licencji wymaganej do rozpowszechniania aplikacji typu fantasy sports.
- Aplikacja musi uniemożliwiać używanie jej w stanach i na terytoriach USA, na terenie których aplikacje typu fantasy sports są nielegalne.

Działania niezgodne z prawem

Zabraniamy publikowania aplikacji umożliwiających lub promujących podejmowanie działań niezgodnych z prawem.

Aby zagwarantować, że platforma Google Play jest bezpiecznym i tolerancyjnym miejscem, stworzyliśmy standardy, które definiują i blokują materiały szkodliwe lub nieodpowiednie dla naszych użytkowników.

- umożliwianie sprzedaży lub zakupu narkotyków;
- przedstawianie albo zachęcanie do używania lub sprzedaży narkotyków, alkoholu bądź tytoniu przez osoby nieletnie;
- instrukcje uprawy nielegalnych roślin lub produkowania narkotyków.

Treści użytkowników

Treści użytkowników to treści umieszczane przez użytkowników w aplikacji, które są widoczne lub dostępne dla co najmniej niektórych spośród użytkowników aplikacji.

Aplikacje, które zawierają lub udostępniają treści generowane przez użytkowników, w tym aplikacje będące specjalistycznymi przeglądarkami lub klientami przekierowującymi użytkowników na platformy z takimi treściami, muszą wdrożyć skuteczne mechanizmy stałego moderowania treści generowanych przez użytkowników, które powinny:

- wymagać, aby użytkownicy zaakceptowali warunki korzystania z aplikacji lub zasady dotyczące użytkowników, zanim będą mogli utworzyć lub przesłać swoje treści;
- definiować kontrowersyjne treści i zachowania (w sposób zgodny z zasadami programu dla deweloperów w Google Play) oraz informować o tym, że są one zabronione, w warunkach korzystania z aplikacji lub zasadach dotyczących użytkowników;
- moderować treści użytkowników stosownie do typu treści umieszczanych przez nich w aplikacji;
  - w przypadku aplikacji do obsługi rzeczywistości rozszerzonej (AR) – moderować treści użytkowników (co obejmuje też system zgłaszania treści w aplikacji) z uwzględnieniem zarówno kontrowersyjnych treści użytkowników (np. obrazów AR o charakterze jednoznacznie seksualnym), jak i kotwiczenia elementów AR w miejscach zastrzeżonych (np. na obszarze o ograniczonym dostępie, takim jak baza wojskowa czy teren prywatny, gdzie zakotwiczenie elementu AR może przysporzyć właścicielowi problemów);
- mieć wbudowany system do zgłaszania kontrowersyjnych treści użytkowników i samych użytkowników oraz podejmowania w związku z nimi odpowiednich działań;
- mieć wbudowany system blokowania treści generowanych przez użytkowników i samych użytkowników;
- mieć zabezpieczenia uniemożliwiające zarabianie na promowaniu nieodpowiedzialnego zachowania użytkowników.

Przypadkowe treści erotyczne

Treści erotyczne są uznawane za „przypadkowe”, jeśli pojawiają się w aplikacji z treściami generowanymi przez użytkowników, która (1) umożliwia dostęp głównie do treści nieerotycznych i (2) nie promuje ani nie poleca aktywnie treści erotycznych. Treści erotyczne uznawane za nielegalne przez obowiązujące przepisy oraz treści narażające dzieci na niebezpieczeństwo nigdy nie są uznawane za „przypadkowe” i są zabronione.

Aplikacje z treściami generowanymi przez użytkowników mogą zawierać przypadkowe treści erotyczne, jeśli spełnione są wszystkie te warunki:

- Treści te są domyślnie ukryte przy pomocy filtrów, których całkowite wyłączenie wymaga wykonania przez użytkownika co najmniej 2 czynności (np. są zasłonięte materiałem pełnoekranowym lub domyślnie wykluczone z wyświetlania, chyba że funkcja „bezpiecznego wyszukiwania” zostanie wyłączona).
- Dzieci, zgodnie z definicją w zasadach dotyczące aplikacji dla rodzin , mają wyraźny zakaz dostępu do aplikacji egzekwowany przez system weryfikacji wieku, taki jak neutralny ekran wyboru wieku lub odpowiedni system wskazany przez obowiązujące przepisy.
- Deweloper aplikacji podał prawidłowe odpowiedzi w kwestionariuszu oceny treści w odniesieniu do treści generowanych przez użytkowników, zgodnie z wymaganiami opisanymi w zasadach oceny treści .

Aplikacje, których głównym celem jest prezentowanie kontrowersyjnych treści użytkowników, będą usuwane z Google Play. Aplikacje, które z biegiem czasu zaczną być używane głównie do zamieszczania kontrowersyjnych treści użytkowników lub zyskają reputację miejsca, w którym takie treści są dostępne, również będą usuwane z Google Play.

Aby zagwarantować, że platforma Google Play jest bezpiecznym i tolerancyjnym miejscem, stworzyliśmy standardy, które definiują i blokują materiały szkodliwe lub nieodpowiednie dla naszych użytkowników.

- Promowanie treści użytkowników o charakterze jednoznacznie seksualnym, m.in. przez implementowanie lub akceptowanie płatnych funkcji, które zachęcają głównie do udostępniania

kontrowersyjnych treści.

- Aplikacje z treściami użytkownika, w przypadku których brakuje odpowiednich zabezpieczeń przed groźbami, nękaniem lub dokuczaniem (zwłaszcza w odniesieniu do osób nieletnich).
- Posty, komentarze lub zdjęcia w aplikacji, których głównym przeznaczeniem jest nękanie lub wyodrębnienie konkretnej osoby w celu znęcania się nad nią, zaatakowania jej lub ośmieszenia.
- Aplikacje, które notorycznie nie reagują na skargi użytkowników dotyczące kontrowersyjnych treści.

Treści i usługi związane ze zdrowiem

Zabraniamy publikowania aplikacji, które prezentują użytkownikom szkodliwe treści i usługi związane ze zdrowiem.

Jeśli Twoja aplikacja zawiera lub promuje treści albo usługi związane ze zdrowiem, musi być zgodna ze wszystkimi obowiązującymi przepisami i regulacjami prawnymi.

Leki na receptę

Zabraniamy publikowania aplikacji umożliwiających sprzedaż lub zakup leków bez recepty.

Niezatwierdzone substancje

Google Play nie dopuszcza aplikacji, które promują lub sprzedają niezatwierdzone substancje, niezależnie od deklaracji na temat ich legalności.

Aby zagwarantować, że platforma Google Play jest bezpiecznym i tolerancyjnym miejscem, stworzyliśmy standardy, które definiują i blokują materiały szkodliwe lub nieodpowiednie dla naszych użytkowników.

- wszystkie pozycje z tego niepełnego wykazu zabronionych leków i suplementów ;
- produkty zawierające efedrynę;
- produkty zawierające gonadotropinę kosmówkową (hCG) przedstawiane w kontekście utraty lub kontroli wagi albo promowane wraz ze sterydami anabolicznymi;
- preparaty ziołowe i suplementy diety zawierające substancję czynną lub niebezpieczne składniki;
- nieprawdziwe lub wprowadzające w błąd oświadczenia zdrowotne, w tym oświadczenia, które sugerują, że produkt jest równie skuteczny jak leki na receptę lub substancje kontrolowane;
- produkty zatwierdzone przez nieoficjalne instytucje, reklamowane tak, aby sugerować bezpieczeństwo i skuteczność w leczeniu oraz profilaktyce określonych chorób i dolegliwości;
- produkty, które były albo są przedmiotem dochodzeń lub ostrzeżeń ze strony urzędów czy instytucji państwowych;
- produkty, których nazwy są łudząco podobne do nazw niezatwierdzonych leków, suplementów lub substancji kontrolowanych.

Więcej informacji o niezatwierdzonych lub błędnie opisanych lekach i suplementach, które monitorujemy, znajdziesz tutaj: www.legitscript.com .

Nieprawdziwe informacje o zdrowiu

Zabraniamy publikowania aplikacji, które zawierają informacje o zdrowiu wprowadzające w błąd, sprzeczne z obecną wiedzą medyczną lub mogące zaszkodzić użytkownikom.

Aby zagwarantować, że platforma Google Play jest bezpiecznym i tolerancyjnym miejscem, stworzyliśmy standardy, które definiują i blokują materiały szkodliwe lub nieodpowiednie dla naszych użytkowników.

- wprowadzające w błąd twierdzenia na temat szczepień, np. że mogą one zmienić czyjeś DNA;
- zachęcanie do szkodliwych, niezatwierdzonych metod leczenia;
- zachęcanie do innych szkodliwych dla zdrowia praktyk, takich jak terapia konwersyjna.

Ograniczenia związane z COVID-19

Aplikacje muszą być zgodne z wymaganiami opisanymi w artykule dotyczącym aplikacji związanych z chorobą koronawirusową 2019 (COVID-19) .

Funkcje medyczne

Nie zezwalamy na aplikacje zawierające funkcje o charakterze medycznym lub związanym ze zdrowiem, które wprowadzają użytkowników w błąd i mogą wyrządzać szkody. Zabraniamy na przykład dodawania aplikacji, które informują, że mają funkcję pulsoksymetru obsługiwaną wyłącznie przez aplikację. Aplikacje pulsoksymetryczne muszą być wspomagane przez urządzenia zewnętrzne, urządzenia do noszenia lub specjalne czujniki w smartfonach zaprojektowane z myślą o obsłudze funkcji pulsoksymetru. Aplikacje wspomagane przez takie urządzenia muszą również mieć w metadanych wyłączenie odpowiedzialności z oświadczeniem, że nie są przeznaczone do użytku medycznego, a jedynie do ogólnych celów treningowych i zdrowotnych, oraz nie są urządzeniami medycznymi, a także muszą mieć prawidłowo podane informacje o zgodnych modelach sprzętu/urządzeń.

Płatności – usługi kliniczne

W przypadku transakcji, które obejmują regulowane usługi kliniczne, nie należy używać systemu rozliczeniowego Google Play. Więcej informacji znajdziesz w artykule o zasadach płatności w Google Play .

Dane pozyskiwane dzięki dostępowi do Health Connect

Dane, do których deweloperzy mają dostęp dzięki uprawnieniom do usługi Health Connect, są uznawane za osobowe i poufne dane użytkownika podlegające zasadom dotyczącym danych użytkownika oraz dodatkowym wymaganiom .

Własność intelektualna

Zabronione jest publikowanie takich aplikacji i tworzenie takich kont dewelopera, które naruszają prawa własności intelektualnej innych podmiotów (w tym znaki towarowe, prawa autorskie, patenty, tajemnice handlowe i pozostałe prawa własności). Niedozwolone są też aplikacje zachęcające lub nakłaniające do naruszania praw własności intelektualnej.

Google reaguje na zrozumiałe zawiadomienia o domniemanym naruszeniu praw autorskich. Aby uzyskać więcej informacji lub złożyć zawiadomienie o naruszeniu ustawy DMCA, zapoznaj się z naszymi procedurami dotyczącymi praw autorskich .

Aby przesłać skargę dotyczącą sprzedaży lub promocji podróbek produktów w aplikacji, prześlij powiadomienie o podróbkach .

Jeśli uważasz, że należący do Ciebie znak towarowy został bezprawnie wykorzystany w aplikacji w Google Play, w celu rozwiązania problemu najpierw powinieneś skontaktować się bezpośrednio z jej deweloperem. Jeśli nie możecie osiągnąć porozumienia, prześlij skargę dotyczącą znaku towarowego za pomocą tego formularza .

Jeśli masz pisemne potwierdzenie, że osoba trzecia wyraziła zgodę na wykorzystanie jej własności intelektualnej w Twojej aplikacji lub na stronie z informacjami o niej (dotyczy to np. nazw i logo marek oraz zasobów graficznych), przed przesłaniem aplikacji skontaktuj się z zespołem Google Play , by uniknąć jej odrzucenia z powodu naruszenia praw własności intelektualnej.

Nieautoryzowane używanie treści chronionych prawem autorskim

Zabronione jest publikowanie aplikacji naruszających prawa autorskie. Modyfikowanie treści chronionych prawem autorskim nadal może skutkować naruszeniem. Aby deweloperzy mogli korzystać z takich treści, możemy poprosić, by udowodnili swoje uprawnienia.

Zachowaj ostrożność, korzystając z treści chronionych prawem autorskim przy prezentowaniu funkcji aplikacji. Zasadniczo najlepszym podejściem jest przygotowanie własnych, oryginalnych materiałów.

Aby zagwarantować, że platforma Google Play jest bezpiecznym i tolerancyjnym miejscem, stworzyliśmy standardy, które definiują i blokują materiały szkodliwe lub nieodpowiednie dla naszych użytkowników.

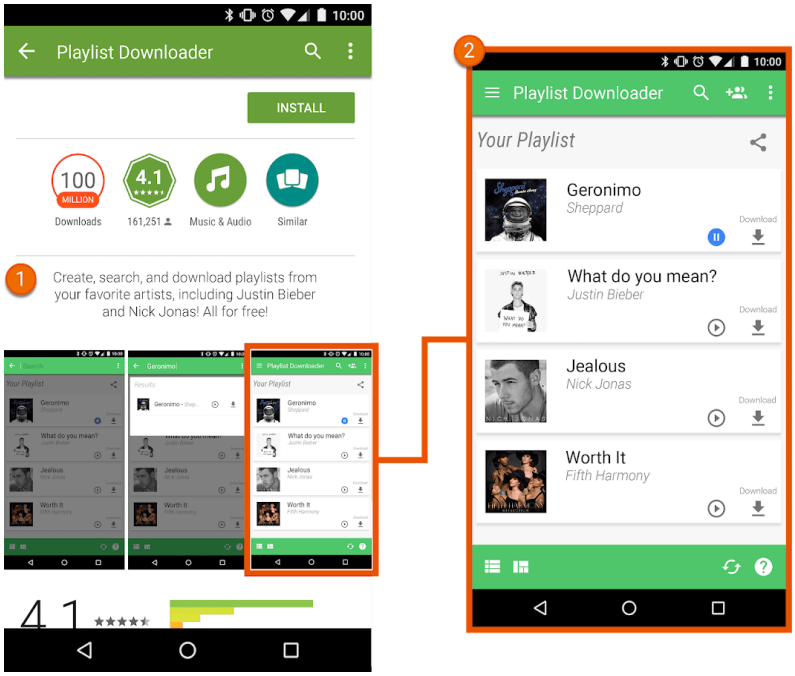
- Okładki albumów muzycznych, gier wideo i książek
- Obrazy marketingowe z filmów, telewizji lub gier wideo
- Plakaty lub obrazy związane z komiksami, kreskówkami, filmami, teledyskami lub telewizją
- Logo uczelni i zawodowych drużyn sportowych
- Zdjęcia skopiowane z konta osoby publicznej w serwisie społecznościowym
- Profesjonalne zdjęcia osób publicznych
- Reprodukcje prac graficznych niemożliwe do odróżnienia od oryginalnych utworów chronionych prawami autorskimi
- Aplikacje z elementami odtwarzającymi klipy dźwiękowe z treści objętych prawami autorskimi
- Pełne kopie lub tłumaczenia książek, które nie należą do domeny publicznej

Zachęcanie do naruszenia praw autorskich

Zabronione jest publikowanie aplikacji nakłaniających lub zachęcających do naruszania praw autorskich. Przed opublikowaniem aplikacji należy zastanowić się, w jaki sposób może ona zachęcać do naruszania praw autorskich, i w razie potrzeby skonsultować się z prawnikiem.

Aby zagwarantować, że platforma Google Play jest bezpiecznym i tolerancyjnym miejscem, stworzyliśmy standardy, które definiują i blokują materiały szkodliwe lub nieodpowiednie dla naszych użytkowników.

- Aplikacje do odtwarzania strumieniowego, które umożliwiają użytkownikom pobranie lokalnej kopii treści chronionych prawami autorskimi bez zezwolenia.
- Aplikacje zachęcające użytkowników do strumieniowania i pobierania utworów objętych prawami autorskimi, w tym muzyki i filmów, które naruszają odpowiednie prawa autorskie.



① Opis w informacjach o tej aplikacji zachęca użytkowników do pobrania bez zezwolenia treści chronionych prawami autorskimi.

② Zrzuty ekranu w informacjach o tej aplikacji zachęcają użytkowników do pobrania bez zezwolenia treści chronionych prawami autorskimi.

Naruszenie praw do znaków towarowych

Zabronione jest publikowanie aplikacji naruszających prawa do znaków towarowych. Znak towarowy to słowo, symbol lub ich połączenie, które określa źródło towaru lub usługi. Właściciel znaku towarowego ma prawo do jego wyłącznego używania razem z określonymi towarami lub usługami.

Naruszenie znaku towarowego to niewłaściwe lub nieautoryzowane użycie identycznego lub podobnego znaku, które może powodować niejasności co do pochodzenia produktu. Jeśli aplikacja korzysta z cudzych znaków towarowych w sposób, który może wprowadzać w błąd, możemy ją zawiesić.

Podróbki

Zabronione jest publikowanie aplikacji, za pomocą których prowadzona jest sprzedaż podróbek produktów lub w których taka sprzedaż jest promowana. Podróbki produktów mają znak towarowy lub logo, które jest identyczne lub niemal identyczne ze znakiem towarowym innego produktu. Naśladują też cechy danej marki, co ma przekonać nabywców, że są to oryginalne wyroby.

Prywatność, oszustwa i używanie urządzeń niezgodnie z przeznaczeniem

Dokładamy wszelkich starań, by chronić prywatność użytkowników i oferować im bezpieczne usługi. Surowo zabraniamy publikowania aplikacji wprowadzających w błąd, złośliwych lub wykorzystujących w nieodpowiedni sposób sieć, urządzenia czy dane osobowe.

Dane użytkownika

Aplikacje muszą w przejrzysty sposób informować o tym, jak są przetwarzane dane użytkownika (np. informacje zbierane od użytkownika, w tym z jego urządzenia). Oznacza to obowiązek informowania o uzyskiwaniu przez aplikację dostępu do danych, ich zbieraniu, używaniu i udostępnianiu. Konieczne jest ograniczenie korzystania z danych tylko do celów zgodnych z ujawnionymi. Jeśli aplikacja obsługuje dane osobowe lub poufne użytkownika, obowiązują dodatkowe wymagania, które zostały wymienione w sekcji „Dane osobowe i poufne” poniżej. Te wymagania Google Play obowiązują jako uzupełnienie przepisów prawa dotyczących ochrony prywatności i danych. Jeśli Twoja aplikacja zawiera kod innej firmy (np. pakiety SDK), musisz dopilnować, aby był on zgodny z Zasadami programu dla deweloperów w Google Play.

Dane osobowe i poufne użytkownika

Dane osobowe i poufne użytkownika obejmują między innymi informacje umożliwiające identyfikację, informacje finansowe i dane związane z płatnościami, dane służące do uwierzytelniania, wpisy z książki telefonicznej, kontakty, dane o lokalizacji urządzenia , SMS-y i dane dotyczące połączeń, dane Health Connect, listę innych aplikacji zainstalowanych na urządzeniu, dane rejestrowane za pomocą mikrofonu i aparatu, a także inne poufne informacje z urządzenia oraz dane o korzystaniu. Jeśli Twoja aplikacja ma dostęp do danych osobowych lub poufnych użytkownika, musisz przestrzegać tych zaleceń:

- Dostęp aplikacji do danych osobowych i poufnych oraz ich zbieranie, używanie i udostępnianie ogranicz do celów bezpośrednio związanych z używaniem i usprawnianiem funkcji tej aplikacji. Mogą to być na przykład funkcje zgodne z przeznaczeniem aplikacji, które są wymienione w jej opisie w Google Play. Udostępnianie danych osobowych i poufnych użytkownika obejmuje używanie pakietów SDK lub innych usług zewnętrznych, które powodują przesyłanie danych do osób trzecich.

Aplikacje, w których korzystanie z danych osobowych i poufnych użytkownika jest poszerzone o wyświetlanie reklam, muszą być zgodne z naszymi zasadami dotyczącymi reklam.

- Ze wszystkimi danymi osobowymi i poufnymi użytkownika postępuj w bezpieczny sposób, używając nowoczesnych metod kryptograficznych (np. protokołu HTTPS).
- Jeśli to możliwe, przed uzyskaniem dostępu do danych objętych uprawnieniami Androida skorzystaj z prośby o pozwolenie na włączenie przy uruchamianiu.
- Nie sprzedawaj danych osobowych ani poufnych użytkowników.

Wymaganie dotyczące informacji dobrze widocznych dla użytkownika oraz uzyskiwania zgody

W przypadkach, w których użytkownicy mogą z uzasadnionych przyczyn nie spodziewać się, że ich dane osobowe lub poufne będą potrzebne do obsługi lub usprawniania zgodnych z zasadami funkcji aplikacji (np. dane są zbierane w tle), musisz spełnić te wymagania:

Zbieranie danych, ich użycie oraz udostępnianie musi zostać wyjaśnione w aplikacji. Informacje wyjaśniające w aplikacji:

- muszą znajdować się w samej aplikacji, a nie tylko w jej opisie czy na stronie internetowej;
- muszą być wyświetlane podczas normalnego używania aplikacji, bez konieczności otwierania menu czy ustawień;
- muszą zawierać opis danych, do których aplikacja ma dostęp lub które zbiera;
- muszą wyjaśniać, jak dane będą używane lub udostępniane;
- nie mogą znajdować się tylko w polityce prywatności lub warunkach usługi;
- nie mogą być częścią innych informacji, które nie dotyczą zbierania danych osobowych lub poufnych użytkowników.

Informacje wyjaśniające postępowanie z danymi w aplikacji muszą wyświetlać się bezpośrednio przed prośbą o zgodę użytkownika i – tam, gdzie ma to zastosowanie – przed powiązaną prośbą o pozwolenie na włączenie przy uruchamianiu. Zabraniamy uzyskiwania dostępu do danych osobowych i poufnych oraz ich zbierania przed uzyskaniem zgody użytkownika. Aplikacja, prosząc o taką zgodę:

- musi w jasny i jednoznaczny sposób prezentować okno z prośbą o zgodę na przetwarzanie danych osobowych,
- musi wymagać wyrażenia zgody w formie działania użytkownika (na przykład kliknięcia przycisku lub zaznaczenia pola wyboru),
- nie może traktować jako zgody opuszczenia przez użytkownika ekranu z tymi informacjami (również przez kliknięcie w innym miejscu aplikacji albo naciśnięcie przycisku Wstecz lub przycisku ekranu głównego),
- do uzyskania zgody nie może stosować komunikatów automatycznie zamykanych ani wygasających.

Aby spełnić wymogi wynikające z zasad, deweloper może w razie potrzeby wykorzystać któryś z zalecanych przez nas przykładowych formatów informacji dobrze widocznych dla użytkowników:

- „[Ta aplikacja] gromadzi/przekazuje/synchronizuje/przechowuje [typ danych], aby umożliwić działanie funkcji [„funkcja”] [w jakich sytuacjach]”.
- *Przykład: „Fitness Funds gromadzi dane o lokalizacji, aby umożliwić działanie funkcji śledzenia aktywności fizycznej nawet wtedy, gdy aplikacja jest zamknięta lub nieużywana, a także aby wyświetlać reklamy”.*
- *Przykład: „Call Buddy gromadzi dane o odczytywaniu i zapisywaniu wpisów w rejestrze połączeń, aby umożliwić działanie funkcji porządkowania kontaktów nawet wtedy, gdy aplikacja jest nieużywana”.*

Aby zagwarantować, że platforma Google Play jest bezpiecznym i tolerancyjnym miejscem, stworzyliśmy standardy, które definiują i blokują materiały szkodliwe lub nieodpowiednie dla naszych użytkowników.

- aplikacja gromadzi dane o lokalizacji urządzenia, ale nie zawiera dobrze widocznych dla użytkowników informacji wyjaśniających, która funkcja używa tych danych, ani wskazujących, że aplikacja działa w tle;
- aplikacja przy uruchomieniu wyświetla prośbę o dostęp do danych, **zanim** wyświetlą się informacje dobrze widoczne dla użytkowników wyjaśniające, do czego mają służyć te dane;
- aplikacja, która ma dostęp do listy aplikacji zainstalowanych przez użytkownika i nie traktuje jej jako danych osobowych ani wrażliwych podlegających polityce prywatności, zasadom postępowania z danymi oraz wymaganiom w zakresie zgody i informacji dobrze widocznych dla użytkowników;
- aplikacja, która ma dostęp do danych z listy kontaktów lub książki telefonicznej i nie traktuje ich jako danych osobowych ani poufnych zgodnie z polityką prywatności, zasadami postępowania z danymi oraz wymaganiami w zakresie zgody i informacji dobrze widocznych dla użytkowników;
- aplikacja, która rejestruje zawartość ekranu na urządzeniu użytkownika i nie traktuje tych danych jako osobowych ani poufnych zgodnie z tymi zasadami;
- aplikacja, która zbiera dane o lokalizacji urządzenia i nie informuje wyczerpująco o sposobie ich użycia ani nie prosi o zgodę na ich użycie, jak nakazują powyższe wymagania;
- aplikacja, która korzysta w tle z uprawnień z ograniczeniami, w tym z uprawnień do śledzenia, prowadzenia badań i marketingu, i nie informuje wyczerpująco o sposobie użycia tych danych ani nie prosi o zgodę na ich użycie, jak nakazują powyższe wymagania.

Ograniczenia dotyczące dostępu do danych osobowych i poufnych

Tabela poniżej zawiera obowiązujące dodatkowo wymagania związane z określonymi czynnościami.

Czynność	Wymaganie
Aplikacja obsługuje informacje finansowe, dane związane z płatnościami lub urzędowe numery identyfikacyjne	Aplikacja nie może nigdy publicznie ujawniać żadnych danych osobowych ani poufnych użytkownika dotyczących finansów, płatności lub urzędowych numerów identyfikacyjnych.
Aplikacja obsługuje niepubliczne informacje z książki telefonicznej lub kontaktów	Nie wolno bez upoważnienia publikować ani ujawniać niepublicznych danych kontaktowych innych osób.
Aplikacja zawiera funkcje antywirusowe, funkcje bezpieczeństwa, np. chroniące przed wirusami i złośliwym oprogramowaniem, lub funkcje zwiększające bezpieczeństwo	Aplikacja musi mieć opublikowaną politykę prywatności, która wraz z innymi objaśnieniami w aplikacji informuje o zakresie zbierania i przekazywania danych użytkownika, sposobie ich użycia oraz o tym, komu są one udostępniane.
Aplikacja jest skierowana do dzieci	Aplikacja nie może zawierać pakietu SDK, który nie został zatwierdzony do użytku w usługach przeznaczonych dla dzieci. Szczegóły dotyczące języka zasad oraz wymagań znajdziesz w artykule Tworzenie aplikacji i gier dla dzieci i rodzin .
Aplikacja zbiera lub łączy trwałe identyfikatory urządzenia (np. IMEI, IMSI, numer seryjny karty SIM itp.)	Zabraniamy łączenia trwałych identyfikatorów urządzenia z danymi osobowymi i poufnymi użytkownika oraz resetowalnymi identyfikatorami urządzeń. Wyjątek stanowią te przypadki: • świadczenie usług telefonicznych powiązanych z kartą SIM (np. do połączeń przez Wi-Fi przypisanych do konta operatora) lub • firmowe aplikacje do zarządzania urządzeniami, które działają w trybie właściciela. Zgodnie z zasadami dotyczącymi danych użytkowników musisz wyraźnie poinformować użytkowników o tych zastosowaniach. Informacje o alternatywnych unikalnych identyfikatorach znajdziesz tutaj . Zapoznaj się z zasadami dotyczącymi reklam , w których znajdują się dodatkowe wytyczne odnośnie do identyfikatora wyświetlania reklam na Androidzie.

Sekcja Bezpieczeństwo danych

Wszyscy deweloperzy muszą podać w sekcji Bezpieczeństwo danych dokładne i jednoznaczne informacje dotyczące każdej aplikacji, wyszczególniając przypadki zbierania, wykorzystywania i udostępniania danych użytkownika. Deweloper odpowiada za prawidłowe oznaczenie i aktualizowanie tych danych. Tam, gdzie ma to zastosowanie, ta sekcja musi być spójna z oświadczeniami zamieszczonymi w polityce prywatności aplikacji.

Więcej informacji o uzupełnianiu sekcji Bezpieczeństwo danych znajduje się w tym artykule .

Polityka prywatności

Wszystkie aplikacje muszą mieć link do polityki prywatności podany w przeznaczonym do tego polu w Konsoli Play oraz link do polityki prywatności lub jej tekst opublikowany w samej aplikacji. Polityka prywatności w połączeniu z innymi objaśnieniami w aplikacji musi wyraźnie informować o tym, w jaki sposób aplikacja uzyskuje dostęp do danych użytkownika oraz jak je zbiera, wykorzystuje i udostępnia. Nie wystarczy wskazanie tych informacji w sekcji Prywatność. Te informacje muszą obejmować:

- dane dewelopera oraz dane osoby do kontaktu w sprawach związanych z prywatnością lub mechanizm przesyłania zapytań;
- rodzaje danych osobowych i wrażliwych użytkownika, do których aplikacja ma dostęp oraz które zbiera, wykorzystuje i udostępnia, a także rodzaje podmiotów, którym udostępniane są takie dane;
- procedury bezpiecznego przetwarzania danych osobowych i wrażliwych użytkownika;
- zasady przechowywania i usuwania danych stosowane przez dewelopera;
- czytelne oznaczenie sekcji jako zawierającej politykę prywatności (np. sformułowanie „polityka prywatności” w tytule).

W polityce prywatności musisz wymienić podmiot (dewelopera lub firmę) wskazany w informacjach o aplikacji w Google Play albo nazwę aplikacji. Politykę prywatności musisz przesłać także w przypadku aplikacji, które nie mają dostępu do żadnych danych osobowych ani wrażliwych użytkowników.

Dopilnuj, aby polityka prywatności znajdowała się pod aktywnym, dostępnym publicznie, niezabezpieczonym przez geofence adresem URL (a nie w pliku PDF) i miała format uniemożliwiający edytowanie.

Wykorzystanie identyfikatora ustawionego przez aplikację

Wprowadzamy na Androidzie nowy identyfikator, który będzie wykorzystywany do obsługi kluczowych przypadków użycia takich jak analizy czy zapobieganie oszustwom. Warunki korzystania z tego identyfikatora znajdują się poniżej.

- **Użycie:** identyfikatora ustawionego przez aplikację nie można używać do personalizacji reklam ani mierzenia ich skuteczności.
- **Powiązanie z informacjami umożliwiającymi identyfikację osoby lub z innymi identyfikatorami:** identyfikatora zestawu aplikacji nie można łączyć w celach reklamowych z żadnymi identyfikatorami Androida (takimi jak AAID) ani innymi danymi osobowymi lub poufnymi.
- **Przejrzystość i uzyskiwanie zgody:** warunki zbierania danych i wykorzystania identyfikatora ustawionego przez aplikację oraz zobowiązanie do ich przestrzegania musisz przedstawić użytkownikom w Informacjach na temat ochrony prywatności. Informacje te muszą być zgodne z przepisami i obejmować także politykę prywatności. W krajach/regionach, w których jest to wymagane, musisz uzyskać wiążącą prawnie zgodę użytkowników. Więcej informacji o naszych standardach ochrony prywatności znajdziesz w zasadach dotyczących danych użytkownika .

EU-U.S., Swiss Privacy Shield (Tarcza Prywatności UE-USA i Szwajcaria-USA)

Jeśli uzyskujesz dostęp do danych osobowych udostępnionych przez Google, korzystasz z nich lub je przetwarzasz, przy czym dane te w sposób pośredni lub bezpośredni umożliwiają identyfikację

określonych osób i pochodzą z Unii Europejskiej lub Szwajcarii („Dane osobowe pochodzące z UE"), musisz:

- Zachować zgodność ze wszystkimi obowiązującymi przepisami prawa, dyrektywami, rozporządzeniami i zasadami dotyczącymi prywatności oraz bezpieczeństwa i ochrony danych.
- Uzyskiwać dostęp do danych osobowych pochodzących z UE oraz korzystać z nich i przetwarzać je tylko w takim celu, na jaki zgadza się osoba, której one dotyczą.
- Stosować odpowiednie środki organizacyjne i techniczne, by zabezpieczyć dane osobowe pochodzące z UE przed ich utratą, użyciem niezgodnym z przeznaczeniem oraz nieautoryzowanym lub nieuprawnionym dostępem, ujawnieniem, modyfikacją bądź zniszczeniem.
- Zapewnić taki sam poziom ochrony, jakiego wymagają zasady programu Privacy Shield (Tarcza Prywatności) .

Masz obowiązek regularnego monitorowania zgodności z wymienionymi warunkami. Jeśli w którymkolwiek momencie utracisz możliwość zachowania zgodności z tymi warunkami lub jeśli wystąpi poważne ryzyko, że tak się stanie, musisz natychmiast powiadomić nas o tym, wysyłając e-maila na adres data-protection-office@google.com , oraz niezwłocznie przerwać przetwarzanie danych osobowych pochodzących z UE lub podjąć uzasadnione i właściwe kroki w celu przywrócenia odpowiedniego poziomu ochrony.

Od 16 lipca 2020 roku nie korzystamy już z programu EU-U.S. Privacy Shield (Tarczy Prywatności UE-USA) do przesyłania danych osobowych pochodzących z Europejskiego Obszaru Gospodarczego lub Wielkiej Brytanii do Stanów Zjednoczonych. Więcej informacjiWięcej informacji znajdziesz w art. 9 Umowy dystrybucyjnej dla deweloperów.

Uprawnienia i interfejsy API z dostępem do informacji poufnych

Prośby dotyczące uprawnień i interfejsów API z dostępem do informacji poufnych powinny być zrozumiałe dla użytkowników. Możesz prosić tylko o uprawnienia i stosowanie interfejsów API z dostępem do informacji poufnych, które są konieczne do zaimplementowania bieżących funkcji lub usług wymienionych w informacjach o aplikacji w Google Play. Nie możesz używać uprawnień ani interfejsów API z dostępem do informacji poufnych, które przyznają dostęp do danych użytkownika lub urządzenia, na potrzeby funkcji lub działań, które są nieujawnione, niezaimplementowane albo niedozwolone. Nigdy nie wolno sprzedawać danych osobowych ani informacji poufnych, do których dostęp jest uzyskiwany po udzieleniu uprawnień lub w ramach interfejsu API z dostępem do informacji poufnych.

W ramach uprawnień i interfejsów API z dostępem do informacji poufnych wyświetlaj prośby o dostęp do danych użytkownika w odpowiednim kontekście (stosując żądania stopniowe). Dzięki temu użytkownicy będą rozumieć, do czego aplikacja potrzebuje konkretnych danych. Dane można wykorzystywać wyłącznie w celach, na które użytkownik wyraził zgodę. Jeśli chcesz użyć danych w innych celach, zapytaj użytkowników, czy zgadzają się na dodatkowe sposoby korzystania z danych i uzyskaj od nich taką zgodę.

Uprawnienia z ograniczeniami

W uzupełnieniu powyższego – uprawnienia z ograniczeniami to takie, które są określane jako niebezpieczne , szczególne lub wymagające podpisu albo są zgodne z poniższym opisem. Podlegają one tym dodatkowym wymaganiom i ograniczeniom:

- Poufne dane użytkownika lub urządzenia, do których uzyskano dostęp na podstawie uprawnień z ograniczeniami, mogą być przekazywane osobom trzecim tylko do zapewnienia działania bieżących funkcji lub usług aplikacji, w której zebrano te dane. Dane można też przekazać w razie potrzeby, gdy jest to wymagane przez obowiązujące prawo albo w ramach fuzji lub przejęcia firmy bądź sprzedaży jej aktywów. Konieczne jest wtedy zgodne z przepisami powiadomienie o tym użytkowników. Inne rodzaje przekazywania lub sprzedaży danych użytkownika są zabronione.

- Jeśli użytkownik odrzuci prośbę o przyznanie uprawnienia z ograniczeniami, musisz uszanować jego decyzję. Nie wolno fałszywie nakłaniać ani zmuszać użytkowników do przyznawania uprawnień, które nie mają krytycznego znaczenia. Musisz podjąć uzasadnione działania, by dostosować funkcjonowanie aplikacji do użytkowników, którzy nie przyznali dostępu do uprawnień newralgicznych (np. umożliwiając ręczne wpisanie numeru telefonu użytkownikowi, który ograniczył dostęp aplikacji do rejestru połączeń).
- Zabronione jest korzystanie z uprawnień w sposób niezgodny z oficjalnymi sprawdzonymi metodami dla deweloperów dotyczącymi uprawnień aplikacji na Androida i obowiązującymi zasadami, takimi jak te związane z nadużywaniem podwyższonych uprawnień).

Niektóre uprawnienia z ograniczeniami są objęte dodatkowymi wymaganiami (szczegóły znajdują się poniżej). Takie ograniczenia mają chronić prywatność użytkownika. W bardzo rzadkich przypadkach możemy zgodzić się na odstępstwa od podanych poniżej wymagań, gdy aplikacja oferuje funkcje, które są bardzo atrakcyjne lub mają znaczenie krytyczne i nie można ich zapewnić w inny sposób. Takie wyjątki rozważamy, biorąc pod uwagę potencjalne zagrożenia dla prywatności i bezpieczeństwa użytkowników.

Uprawnienia dostępu do SMS-ów i rejestru połączeń

Uprawnienia dostępu do SMS-ów i rejestru połączeń są traktowane jako osobowe i poufne dane użytkownika. Podlegają zasadom opisanym w sekcji Dane osobowe i poufne oraz tym ograniczeniom:

Uprawnienia z ograniczeniami	Wymaganie
Grupa uprawnień Rejestr połączeń (np. READ_CALL_LOG, WRITE_CALL_LOG, PROCESS_OUTGOING_CALLS)	Musi być aktywnie zarejestrowana jako domyślna aplikacja telefonu lub pomocnicza na urządzeniu.
Grupa uprawnień SMS (np. READ_SMS, SEND_SMS, WRITE_SMS, RECEIVE_SMS, RECEIVE_WAP_PUSH, RECEIVE_MMS)	Musi być aktywnie zarejestrowana jako domyślna aplikacja do obsługi SMS-ów lub Asystenta na urządzeniu.

Aplikacje, których nie można ustawić jako domyślnej aplikacji do obsługi SMS-ów, telefonu lub Asystenta, nie mogą deklarować korzystania z powyższych uprawnień w manifeście. Obejmuje to tekst zastępczy w manifeście. Poza tym, zanim aplikacja wyświetli użytkownikowi prośbę o zaakceptowanie dowolnego z powyższych uprawnień, musi być aktywnie zarejestrowana jako domyślna aplikacja do obsługi SMS-ów, telefonu lub Asystenta. Musi też niezwłocznie przestać korzystać z danego uprawnienia, gdy straci status domyślnej aplikacji do obsługi. Dozwolone przypadki użycia i wyjątki są opisane na tej stronie w Centrum pomocy .

Aplikacja może korzystać z uprawnienia (i dowolnych danych uzyskanych na jego podstawie) wyłącznie do udostępniania swoich zatwierdzonych, kluczowych funkcji. Kluczowa funkcja to podstawowe przeznaczenie aplikacji. Może to być zestaw podstawowych funkcji, z których każda musi być w widoczny sposób udokumentowana i wskazana w opisie aplikacji. Aplikacja bez kluczowych funkcji jest uważana za „zepsutą”, czyli bezużyteczną. Przesyłanie, udostępnianie lub licencjonowane użycie tych danych może odbywać się wyłącznie w związku z zapewnianiem działania kluczowych funkcji i usług aplikacji. Nie wolno używać tych danych do innych celów (np. usprawniania innych aplikacji lub usług bądź w celach marketingowych). Do odczytywania danych uzyskiwanych na podstawie uprawnień dostępu do rejestru połączeń lub SMS-ów nie wolno używać alternatywnych rozwiązań (w tym innych uprawnień, interfejsów API ani zewnętrznych źródeł danych).

Dostęp do lokalizacji

Lokalizacja urządzenia uznawana jest za dane osobowe i poufne użytkownika podlegające zasadom dotyczącym danych osobowych i informacji poufnych , zasadom dotyczącym lokalizacji w tle oraz tym wymogom:

- Aplikacja nie może korzystać z danych wymagających dostępu do lokalizacji (np. ACCESS_FINE_LOCATION, ACCESS_COARSE_LOCATION czy ACCESS_BACKGROUND_LOCATION), które nie są już konieczne do udostępniania bieżących funkcji lub usług aplikacji.
- Aplikacja nie powinna nigdy prosić użytkowników o dostęp do lokalizacji, jeśli ma to służyć tylko do wyświetlania reklam lub analizy danych. Aplikacje, w których dozwolone użycie tych danych jest poszerzone o wyświetlanie reklam, muszą być zgodne z naszymi zasadami dotyczącymi reklam .
- Aplikacje powinny prosić o przyznanie dostępu na najniższym poziomie (np. do przybliżonej lokalizacji zamiast dokładnej, na pierwszym planie zamiast w tle) niezbędnym do zapewnienia działania funkcji lub usługi, która wymaga danych o lokalizacji. Użytkownicy powinni spodziewać się, że ta funkcja lub usługa potrzebuje żądanego poziomu dostępu do lokalizacji. Możemy odrzucić aplikacje, które proszą o dostęp do lokalizacji w tle lub z niej korzystają bez wystarczającego uzasadnienia.
- Lokalizacji w tle można używać wyłącznie do udostępniania użytkownikowi funkcji przynoszących mu korzyści i ściśle związanych z podstawowym przeznaczeniem aplikacji.

Aplikacja może korzystać z dostępu do lokalizacji jako usługa działająca na pierwszym planie (gdy aplikacja ma dostęp tylko na pierwszym planie, np. „podczas używania"), jeśli takie użycie:

- jest kontynuacją wywołanego przez użytkownika działania w aplikacji,
- zostaje zakończone natychmiast po prawidłowym wykonaniu przez aplikację działania wywołanego przez użytkownika.

Aplikacje przeznaczone dla dzieci muszą być zgodne z zasadami programu Dla całej rodziny .

Więcej informacji o wymaganiach wynikających z tych zasad znajdziesz w tym artykule pomocy .

Uprawnienia dostępu do wszystkich plików

Atrybuty plików i katalogów na urządzeniu użytkownika są traktowane jako osobowe i poufne dane użytkownika. Podlegają zasadom opisanym w sekcji Dane osobowe i poufne oraz tym ograniczeniom:

- Aplikacje powinny prosić o dostęp do pamięci urządzenia, jeśli jest on niezbędny do działania aplikacji, i nie mogą prosić o dostęp do pamięci urządzenia w imieniu osób trzecich w żadnym celu niezwiązanym z niezbędnymi, widocznymi dla użytkownika funkcjami aplikacji.
- Urządzenia z Androidem w wersji R lub nowszej wymagają uprawnień MANAGE_EXTERNAL_STORAGE , by zarządzać dostępem w pamięci współdzielonej. Wszystkie aplikacje kierowane na Androida R i żądające szerokiego dostępu do pamięci współdzielonej („Dostęp do wszystkich plików") muszą przed opublikowaniem pomyślnie przejść odpowiednią kontrolę dostępu. Aplikacje, które mogą korzystać z tych uprawnień, muszą wyraźnie informować użytkowników o włączeniu opcji „Dostęp do wszystkich plików" w ustawieniach „Aplikacje ze specjalnym dostępem". Więcej informacji o wymaganiach dotyczących Androida R znajdziesz w tym artykule w Centrum pomocy .

Uprawnienia do wyświetlania pakietów (aplikacji)

Lista zainstalowanych aplikacji pobierana z urządzenia jest traktowana jako osobowe i poufne dane użytkownika. Podlega ona zasadom dotyczącym danych osobowych i poufnych oraz tym ograniczeniom:

Aplikacje, których podstawowym celem jest uruchamianie innych aplikacji zainstalowanych na urządzeniu, wyszukiwanie ich i współdziałanie z nimi, mogą mieć wgląd w inne aplikacje na tych zasadach:

- **Duża widoczność aplikacji:** aplikacja ma szeroki wgląd w zainstalowane aplikacje („pakiety") na urządzeniu.
  - W przypadku aplikacji używających interfejsu API na poziomie 30 lub nowszym duża widoczność zainstalowanych aplikacji oparta na uprawnieniu QUERY_ALL_PACKAGES jest

ograniczona do konkretnych przypadków użycia – gdy aplikacja wymaga do działania informacji o aplikacjach lub współdziałania z niektórymi lub wszystkimi aplikacjami na urządzeniu.
    - Nie możesz używać uprawnienia QUERY_ALL_PACKAGES, jeśli aplikacja może działać z bardziej szczegółową deklaracją widoczności pakietów , np. gdy wyszukuje określone pakiety i wchodzi z nimi w interakcje, zamiast wysyłać prośby o dużą widoczność.
  - Możliwość korzystania z alternatywnych metod szacowania dużej widoczności powiązanej z uprawnieniem QUERY_ALL_PACKAGES również jest ograniczona do podstawowych funkcji aplikacji dostępnych dla użytkowników i współdziałania z aplikacjami wykrytymi za pomocą tej metody.
  - Dozwolone przypadki użycia uprawnienia QUERY_ALL_PACKAGES znajdziesz w tym artykule w Centrum pomocy .
- **Ograniczona widoczność aplikacji:** aplikacja maksymalnie ogranicza dostęp do danych, wyszukując określone aplikacje za pomocą bardziej precyzyjnych metod (np. wysyła zapytania dotyczące konkretnych aplikacji, które spełniają wymagania deklaracji w pliku manifestu). Tej metody możesz używać do wysyłania zapytań dotyczących aplikacji, gdy Twoja aplikacja współdziała z tymi aplikacjami lub nimi zarządza zgodnie z zasadami.
- Widoczność zasobów reklamowych aplikacji zainstalowanych na urządzeniu musi być bezpośrednio związana z głównym przeznaczeniem lub podstawową funkcją, z której korzystają ich użytkownicy.

Dane o zasobach aplikacji rozpowszechnianych w Google Play nie mogą być sprzedawane ani udostępniane na potrzeby analityki i zarabiania na reklamach.

Accessibility API

Za pomocą interfejsu Accessibility API nie można:

- zmieniać ustawień użytkownika bez jego zgody ani uniemożliwiać użytkownikowi wyłączenia lub odinstalowania jakiejkolwiek aplikacji bądź usługi, chyba że za zgodą rodzica lub opiekuna wyrażonej w aplikacji do kontroli rodzicielskiej lub za zgodą upoważnionego administratora w ramach oprogramowania do zarządzania w firmach;
- obchodzić wbudowanych w Androida ustawień prywatności ani powiadomień;
- zmieniać ani wykorzystywać interfejsu w sposób, który wprowadza w błąd lub narusza zasady dla deweloperów w Google Play.

Interfejs Accessibility API nie służy do zdalnego nagrywania dźwięku połączeń i nie może być do tego używany.

Korzystanie z interfejsu Accessibility API musi być udokumentowane w informacjach o aplikacji w Google Play.

Wytyczne dotyczące atrybutu IsAccessibilityTool

Aplikacje, których podstawowym przeznaczeniem jest bezpośrednie wspieranie osób z niepełnosprawnościami, mogą za pomocą atrybutu **IsAccessibilityTool** publicznie zaznaczyć, że są aplikacjami ułatwień dostępu.

Aplikacje, które nie kwalifikują się do korzystania z atrybutu **IsAccessibilityTool**, nie mogą używać tej flagi. Muszą też spełniać wymagania w zakresie wyraźnego informowania i uzyskiwania zgody na gromadzenie informacji, jak opisano w zasadach dotyczących danych użytkownika , ponieważ ich funkcje związane z ułatwieniami dostępu nie są oczywiste dla odbiorcy. Więcej informacji znajdziesz w Centrum pomocy, w artykule dotyczącym interfejsu AccessibilityService API .

Gdy to możliwe, zamiast interfejsu Accessibility API aplikacje muszą korzystać z bardziej ograniczonych uprawnień i interfejsów API , aby zapewnić oczekiwane działanie.

Prośba o uprawnienia do instalowania pakietów

Uprawnienie REQUEST_INSTALL_PACKAGES umożliwia aplikacji żądanie zainstalowania jej pakietów. Aby aplikacja mogła z niego skorzystać, jej główna funkcja musi obejmować:

- wysyłanie lub odbieranie pakietów aplikacji,
- umożliwianie instalowania przez użytkownika pakietów aplikacji.

Dozwolone funkcje to:

- przeglądanie stron lub wyszukiwanie w internecie;
- usługi komunikacyjne, które obsługują załączniki;
- udostępnianie lub transfer plików albo zarządzanie nimi;
- zarządzanie urządzeniami firmowymi;
- tworzenie i przywracanie kopii zapasowej;
- migracja danych z urządzenia / przenoszenie danych z telefonu.

Główna funkcja to ogólne przeznaczenie aplikacji. Główna funkcja, a także wszelkie ważne funkcje, które się na nią składają, muszą być w widoczny sposób udokumentowane i umieszczone w opisie aplikacji.

Uprawnienie REQUEST_INSTALL_PACKAGES nie może być wykorzystywane do przeprowadzania samoaktualizacji, wprowadzania modyfikacji ani do łączenia w pakiety innych plików APK w pliku zasobów w celach innych niż zarządzanie urządzeniem. Wszystkie aktualizacje i instalacje pakietów muszą być zgodne z zasadami Google Play dotyczącymi nadużywania urządzeń lub sieci , a także muszą być inicjowane przez użytkownika.

Uprawnienia Health Connect by Android

Dane, do których deweloperzy uzyskują dostęp przy użyciu uprawnień Health Connect, są uznawane za osobowe i poufne dane użytkownika podlegające zasadom dotyczącym danych użytkownika oraz tym dodatkowym wymaganiom:

Uzyskiwanie dostępu do danych Health Connect i korzystanie z nich w odpowiedni sposób

Prośby o dostęp do danych z Health Connect muszą być jasne i zrozumiałe. Z Health Connect można korzystać tylko zgodnie z odpowiednimi zasadami i Warunkami korzystania z usługi oraz tylko w zatwierdzonych przypadkach użycia określonych w tych zasadach. Oznacza to, że można prosić o uprawnienia tylko wtedy, gdy aplikacja lub usługa jest zgodna z jednym z zatwierdzonych przypadków użycia.

Zatwierdzone przypadki użycia pozwalające na dostęp do uprawnień Health Connect:

- Aplikacje lub usługi z co najmniej 1 funkcją zapewniającą użytkownikom korzyści związane ze zdrowiem i aktywnością fizyczną za pomocą interfejsu, który umożliwia bezpośrednie **rejestrowanie, raportowanie, monitorowanie lub analizowanie** danych o aktywności fizycznej, śnie, stanie psychicznym lub odżywianiu, pomiarów parametrów zdrowotnych, opisów fizycznych bądź innych opisów i pomiarów związanych ze zdrowiem lub aktywnością fizyczną.
- Aplikacje lub usługi z co najmniej 1 funkcją zapewniającą użytkownikom korzyści związane ze zdrowiem i aktywnością fizyczną za pomocą interfejsu, który umożliwia **przechowywanie** na urządzeniu do noszenia lub telefonie danych o aktywności fizycznej, śnie, stanie psychicznym lub odżywianiu, pomiarów parametrów zdrowotnych, opisów fizycznych bądź innych opisów i pomiarów związanych ze zdrowiem lub aktywnością fizyczną, a także udostępnianie tych danych innych aplikacjom na urządzeniu, które spełniają wymogi dopuszczonych przypadków użycia.

Health Connect to platforma ogólnego przeznaczenia do przechowywania i udostępniania danych, która pozwala użytkownikom na agregowanie danych o zdrowiu i kondycji fizycznej z różnych źródeł na posiadanym urządzeniu z Androidem oraz dobrowolne udostępnianie ich osobom trzecim. Dane mogą pochodzić z różnych źródeł określonych przez użytkowników. Deweloperzy muszą ocenić, czy Health Connect jest odpowiednią platformą na ich potrzeby, a także sprawdzić i dokładnie ocenić

źródło oraz jakość danych z Health Connect, a także ich przydatność do zamierzonego celu, zwłaszcza w kontekście badań, zdrowia lub medycyny.

- Aplikacje służące do prowadzenia badań związanych ze zdrowiem osób, korzystające z danych uzyskanych przez Health Connect, muszą uzyskać zgodę od uczestników, a w przypadku osób nieletnich – od ich rodziców lub opiekunów. Taka zgoda musi zawierać te informacje: (a) charakter, cel i czas trwania badania; (b) procedury, ryzyko i korzyści dla uczestnika; (c) informacje na temat poufności danych i postępowania z nimi (w tym udostępniania ich osobom trzecim); (d) dane osoby kontaktowej, do której uczestnicy mogą kierować pytania; (e) proces rezygnacji z udziału w badaniu. Aplikacje służące do prowadzenia badań związanych ze zdrowiem osób, korzystające z danych uzyskanych przez Health Connect, muszą być zatwierdzone przez niezależny organ, który: 1) ma za zadanie chronić prawa, bezpieczeństwo i zdrowie uczestników; 2) ma uprawnienia do kontrolowania, modyfikowania i zatwierdzania badań z udziałem osób. Deweloper musi dysponować potwierdzeniem zgody wydanej przez taki organ i przedstawić go na żądanie.
- Deweloper odpowiada także za zapewnienie zgodności z wszelkimi przepisami i wymaganiami prawnymi, które mogą obowiązywać w przypadku zamierzonego wykorzystania Health Connect oraz wszelkich danych z tej platformy. Z wyjątkiem informacji jednoznacznie podanych na oznaczeniach lub w opisach konkretnych usług Google, Google nie promuje ani nie gwarantuje poprawności żadnych danych przechowywanych w Health Connect, a także nie gwarantuje ich użyteczności w żadnym celu, zwłaszcza w kontekście badań, zdrowia lub medycyny. Google w pełni wyłącza swoją odpowiedzialność za korzystanie z danych uzyskanych przez Health Connect.

Ograniczone użytkowanie

W ramach dopuszczalnego korzystania z Health Connect deweloperzy muszą zagwarantować, że użycie przez nich danych z Health Connect spełnia także poniższe wymogi. Dotyczą one nieprzetworzonych danych uzyskanych z Health Connect oraz danych zbiorczych, zdeidentyfikowanych lub pozyskanych z nieprzetworzonych danych.

- Deweloperzy powinni ograniczyć wykorzystanie danych z Health Connect tak, aby używać ich wyłącznie w ramach dopuszczalnego użytkowania lub realizowania funkcji dobrze widocznych w interfejsie aplikacji żądającej dostępu do tych danych.
- Dane użytkowników można przekazywać osobom trzecim wyłącznie w tych przypadkach:
  - w ramach dopuszczalnego użytkowania lub realizowania funkcji, które są jasno określone w interfejsie aplikacji żądającej dostępu do tych danych, i wyłącznie za zgodą użytkownika;
  - jeśli jest to niezbędne ze względów bezpieczeństwa (na przykład do badania przypadków nadużyć);
  - jeśli jest to konieczne w celu zastosowania się do obowiązujących przepisów;
  - w wyniku fuzji, przejęcia lub sprzedaży aktywów dewelopera, po uzyskaniu wcześniej wyraźnej zgody użytkownika.
- Zabronione jest odczytywanie danych użytkownika przez inne osoby, z wyjątkiem tych sytuacji:
  - deweloper uzyskał wyraźną zgodę użytkownika na odczytanie określonych danych;
  - jest to niezbędne ze względów bezpieczeństwa (na przykład do badania przypadków nadużyć);
  - jest to konieczne w celu zastosowania się do obowiązujących przepisów;
  - dane (oraz ich pochodne) są agregowane i używane wewnętrznie zgodnie z odpowiednimi zasadami zachowania prywatności oraz innymi wymaganiami prawnymi w danej jurysdykcji.

Wszelkie inne przypadki przekazywania, wykorzystywania lub sprzedawania danych z Health Connect są zabronione. Ten zakaz obejmuje:

- przekazywanie lub sprzedawanie danych użytkownika osobom trzecim, na przykład platformom reklamowym, brokerom danych czy jakimkolwiek innym podmiotom zajmującym się handlem danymi;
- przekazywanie, sprzedawanie lub wykorzystywanie danych użytkownika do wyświetlania reklam, w tym reklam spersonalizowanych i opartych na zainteresowaniach;

- przekazywanie, sprzedawanie lub wykorzystywanie danych użytkownika do określenia zdolności kredytowej lub na inne potrzeby związane z udzielaniem pożyczek;
- przekazywanie, sprzedawanie lub wykorzystywanie danych użytkownika na potrzeby innego produktu lub usługi, które mogą kwalifikować się jako urządzenie medyczne według definicji w sekcji 201(h) Federalnej ustawy o żywności, lekach i kosmetykach (Federal Food Drug & Cosmetic Act), jeśli dane użytkownika będą używane przez urządzenie medyczne do wykonywania jego przewidzianej prawnie funkcji.
- przekazywanie, sprzedawanie lub wykorzystywanie danych użytkownika do jakiegokolwiek celu lub w jakikolwiek sposób związany z chronionymi informacjami zdrowotnymi (PHI, zgodnie z definicją HIPAA), chyba że deweloper otrzyma wcześniej od Google pisemną zgodę na takie użycie.

Dostęp do Health Connect nie może być realizowany w sprzeczności z tymi zasadami lub jakimikolwiek innymi obowiązującymi przepisami lub Warunkami korzystania z Health Connect. Obejmuje to te cele:

- Nie wolno używać Health Connect do tworzenia aplikacji, środowisk lub aktywności (ani jako dodatku do nich), jeśli istnieje uzasadnione ryzyko, że wykorzystanie danych z Health Connect lub wadliwe działanie tej platformy może doprowadzić do śmierci, obrażeń, szkód środowiskowych lub zniszczenia mienia (na przykład na potrzeby konstruowania i eksploatowania zakładów jądrowych, systemów kierowania ruchem lotniczym, systemów podtrzymywania życia czy uzbrojenia).
- Nie wolno uzyskiwać dostępu do danych zebranych przez Health Connect za pomocą aplikacji bez interfejsu graficznego. Aplikacje muszą wyświetlać łatwo rozpoznawalną ikonę w panelu aplikacji, ustawieniach aplikacji na urządzeniu, ikonach powiadomień itp.
- Nie wolno używać Health Connect z aplikacjami, które synchronizują dane między niezgodnymi urządzeniami lub platformami.
- Health Connect nie można łączyć z aplikacjami, usługami ani funkcjami kierowanymi wyłącznie do dzieci. Platforma Health Connect nie została zatwierdzona do używania w usługach skierowanych głównie do dzieci.

W aplikacji lub na stronie internetowej powiązanej z usługą sieciową lub aplikacją deweloper musi zamieścić oświadczenie, że wykorzystywanie przez niego danych z Health Connect jest zgodne z wymogami ograniczonego użycia. Może to być na przykład link na stronie głównej kierujący do odpowiedniej strony lub polityki prywatności z informacją: „Wykorzystanie informacji uzyskanych z Health Connect będzie zgodne z zasadami uprawnień do Health Connect, w tym z wymogami ograniczonego użytkowania”.

Dane w minimalnym zakresie

Można prosić o dostęp tylko do tych uprawnień, które są niezbędne do realizowania funkcji aplikacji lub usługi.

Oznacza to, że:

- Nie należy prosić o dostęp do informacji, których się nie potrzebuje. Należy prosić o dostęp wyłącznie do uprawnień niezbędnych do zaimplementowania usług lub funkcji produktu. Jeśli produkt nie wymaga dostępu do określonych uprawnień, nie wolno prosić użytkownika o ich przyznanie.

Przejrzyste i precyzyjne metody powiadamiania i kontroli

Health Connect obsługuje dane o zdrowiu i aktywności fizycznej, w tym osobowe i poufne informacje. Wszystkie aplikacje i usługi muszą zawierać politykę prywatności, która musi w pełni opisywać, w jaki sposób dana aplikacja lub usługa zbiera, wykorzystuje i udostępnia dane użytkownika. Obejmuje to informacje o osobach trzecich, którym udostępniane są dane użytkownika, o sposobie wykorzystywania, przechowywania i zabezpieczania danych przez dewelopera, a także o tym, co się dzieje z danymi w przypadku dezaktywacji lub usunięcia konta.

Oprócz wymagań wynikających z obowiązującego prawa, deweloper musi także stosować się do tych wymogów:

- Należy wyjaśnić proces uzyskiwania dostępu do danych, ich użycia oraz udostępniania. W tym wyjaśnieniu:
  - należy dokładnie wskazać aplikację lub usługę, która wymaga dostępu do danych użytkownika;
  - należy podać jasne i dokładne informacje o typach danych, do których aplikacja lub usługa uzyskuje dostęp, o które prosi lub które zbiera;
  - należy przekazać, jak dane będą używane lub udostępniane: jeśli deweloper wymaga dostępu do danych z jednego powodu, ale będą one wykorzystywane też w innym celu, musi on poinformować użytkowników o obydwu przypadkach użycia.
- należy zapewnić użytkownikom dostęp do dokumentacji pomocy, w której wyjaśnione będzie, jak mogą oni zarządzać swoimi danymi w aplikacji i jak je usuwać.

Bezpieczna obsługa danych

Postępowanie z danymi użytkownika musi odbywać się w bezpieczny sposób. Deweloper musi podjąć wszelkie odpowiednie kroki w celu zabezpieczenia wszystkich aplikacji lub systemów korzystających z Health Connect przed nieautoryzowanym lub bezprawnym dostępem, użyciem, zniszczeniem, utratą, zmianą lub ujawnieniem danych.

Wśród zalecanych środków bezpieczeństwa jest zaimplementowanie i utrzymywanie systemu zarządzania bezpieczeństwem informacji, tak jak opisano to w normie ISO/IEC 27001, oraz zapewnienie, że aplikacja lub usługa sieciowa nie ma typowych luk w zabezpieczeniach, tak jak opisano to w publikacji OWASP Top 10.

W zależności od wykorzystywanego interfejsu API oraz liczby użytkowników wymagamy od deweloperów, aby ich aplikacje lub usługi poddawane były okresowej ocenie bezpieczeństwa oraz uzyskały list oceniający od wyznaczonej do tego organizacji, jeśli ich produkt wysyła dane poza urządzenie użytkownika.

Więcej informacji na temat wymagań wobec aplikacji łączących się z Health Connect można znaleźć w tym artykule pomocy.

Usługa VPN

VpnService to klasa bazowa, która umożliwia Twoim aplikacjom rozszerzanie i tworzenie własnych rozwiązań VPN. Tylko aplikacje używające VpnService i mające VPN jako główną funkcję mogą tworzyć na poziomie urządzenia bezpieczne tunele do serwera zdalnego. Do wyjątków należą aplikacje, które wymagają serwera zdalnego do obsługi swoich głównych funkcji, na przykład:

- aplikacje do kontroli rodzicielskiej i aplikacje do zarządzania;
- śledzenie użytkowania aplikacji;
- aplikacje zabezpieczające urządzenie (np. antywirusy, aplikacje do zarządzania urządzeniami mobilnymi, zapory sieciowe);
- narzędzia związane z siecią (na przykład do dostępu zdalnego);
- aplikacje do przeglądania internetu;
- aplikacje operatora, które wymagają sieci VPN, aby umożliwić dostęp do usług telefonicznych lub komunikacyjnych.

Klasy VpnService nie można używać do:

- zbierania danych osobowych i wrażliwych użytkowników bez podania dobrze widocznej informacji i uzyskania zgody;
- przekierowywania lub modyfikowania ruchu użytkowników z innych aplikacji na urządzeniu na potrzeby generowania przychodu (na przykład przekierowywania ruchu z reklam przez kraj inny niż kraj użytkownika);
- manipulowania reklamami, które mogą wpływać na zarabianie na aplikacji.

Aplikacje używające klasy VpnService muszą:

- mieć informację o używaniu VpnService na swojej stronie w Google Play;
- szyfrować dane przechodzące z urządzenia do punktu końcowego tunelu VPN;
- przestrzegać wszystkich zasad programu dla deweloperów , w tym zasad dotyczących oszustw reklamowych , uprawnień i złośliwego oprogramowania .

Zmiany obowiązujące od 31 lipca 2023 roku

Uprawnienie dostępu do precyzyjnych alarmów

Wprowadzimy nowe uprawnienie USE_EXACT_ALARM, które będzie dawało dostęp do funkcji precyzyjnego alarmu w aplikacjach na Androidzie w wersji od 13 wzwyż (docelowy poziom API 33).

USE_EXACT_ALARM to uprawnienie z ograniczonym dostępem, które aplikacje mogą deklarować wyłącznie wtedy, gdy ich główna funkcja wymaga precyzyjnego alarmu. Aplikacje, które proszą o to uprawnienie, są weryfikowane, a te, które nie spełniają kryteriów dopuszczalnego użytkowania, nie mogą być publikowane w Google Play.

Zasady dopuszczalnego użytkowania uprawnienia dostępu do precyzyjnych alarmów

Aplikacja może używać uprawnienia USE_EXACT_ALARM tylko wtedy, gdy jej główna, widoczna dla użytkowników funkcja wymaga wykonywania działań w precyzyjnym czasie. Na przykład:

- Aplikacja to budzik lub stoper.
- Aplikacja to kalendarz, który wyświetla powiadomienia o wydarzeniach.

Jeśli Twój przypadek użycia funkcji precyzyjnego alarmu nie został opisany powyżej, zastanów się, czy nie można w tym przypadku użyć uprawnienia SCHEDULE_EXACT_ALARM.

Więcej informacji o funkcji precyzyjnego alarmu znajdziesz w tym przewodniku dla deweloperów .

Nadużywanie urządzenia lub sieci

Zabraniamy publikowania aplikacji, które zakłócają działanie lub powodują uszkodzenie urządzenia użytkownika, innych urządzeń bądź komputerów, serwerów, sieci, interfejsów API czy usług albo uzyskują do nich nieautoryzowany dostęp. Dotyczy to m.in. innych aplikacji na urządzeniu, wszelkich usług Google i autoryzowanych sieci operatorów komórkowych.

Aplikacje w Google Play muszą spełniać domyślne wymagania optymalizacji pod względem działania w systemie Android opisane w kluczowych wytycznych dotyczących jakości aplikacji w Google Play .

Aplikacja rozpowszechniana w Google Play nie może samodzielnie się modyfikować, zastępować ani aktualizować przy użyciu metody innej niż mechanizm aktualizacji Google Play. Aplikacja nie może też pobierać kodu wykonywalnego (np. plików .dex, .jar i .so) z innego źródła niż Google Play. Nie dotyczy to kodu, który jest uruchamiany na maszynie wirtualnej czy w interpreterze z pośrednim dostępem do interfejsów API Androida (na przykład JavaScript w komponencie WebView lub przeglądarce).

Aplikacje lub kod innej firmy (np. SDK) z interpretowanymi językami (JavaScript, Python, Lua itp.) ładowanymi podczas działania (np. niespakowanymi z aplikacją) nie mogą dopuszczać do potencjalnych naruszeń zasad Google Play.

Zabraniamy wykorzystywania kodu, który wprowadza lub wykorzystuje luki w zabezpieczeniach. Zapoznaj się z naszym Programem ulepszania zabezpieczeń aplikacji , aby dowiedzieć się, jakie problemy z zabezpieczeniami zostały ostatnio zgłoszone deweloperom.

Wymagania dotyczące ustawienia Flag Secure

FLAG_SECURE to flaga wyświetlania deklarowana w kodzie aplikacji w celu wskazania, że UI zawiera dane wrażliwe, które mają być ograniczane do bezpiecznej platformy podczas używania aplikacji. Flaga powstała po to, aby zapobiegać pojawianiu się danych na zrzutach ekranów i ich wyświetlaniu na niezabezpieczonych wyświetlaczach. Deweloperzy deklarują tę flagę, jeśli treść aplikacji nie

powinna być upubliczniana, wyświetlana ani w inny sposób przekazywana poza aplikację i urządzenie użytkownika.

Ze względów bezpieczeństwa i prywatności wszystkie aplikacje rozpowszechnianie w Google Play muszą przestrzegać deklaracji FLAG_SECURE innych aplikacji. Oznacza to, że aplikacje nie mogą umożliwiać ani tworzyć obejścia ustawień FLAG_SECURE innych aplikacji.

Aplikacje, które kwalifikują się jako narzędzia ułatwień dostępu , nie muszą przestrzegać tego wymagania pod warunkiem, że nie przekazują, nie zapisują ani nie przechowują w pamięci podręcznej treści chronionych ustawieniem FLAG_SECURE w sposób umożliwiający dostęp do tych treści poza urządzeniem użytkownika.

Aby zagwarantować, że platforma Google Play jest bezpiecznym i tolerancyjnym miejscem, stworzyliśmy standardy, które definiują i blokują materiały szkodliwe lub nieodpowiednie dla naszych użytkowników.

- aplikacje blokujące lub zakłócające działanie innych aplikacji wyświetlających reklamy;
- aplikacje do oszukiwania w grach, które wpływają na rozgrywkę w innych aplikacjach;
- aplikacje umożliwiające hakowanie usług, oprogramowania lub sprzętu albo omijanie zabezpieczeń lub aplikacje zawierające instrukcje wykonania tych czynności;
- aplikacje mające dostęp do usług lub interfejsów API albo używające ich w sposób niezgodny z ich warunkami korzystania;
- aplikacje próbujące obejść systemowe zarządzanie energią , które nie kwalifikują się do umieszczenia na białej liście ;
- aplikacje umożliwiające dostęp do innych usług przez serwery proxy mogą działać w ten sposób tylko wtedy, gdy jest to ich główna funkcja widoczna dla użytkowników;
- aplikacje lub kod innej firmy (np. pakiety SDK) pobierające kod wykonywalny (np. pliki .dex lub kod natywny) ze źródła innego niż Google Play;
- aplikacje instalujące inne aplikacje na urządzeniu bez uprzedniej zgody użytkownika;
- aplikacje z linkami prowadzącymi do instalatorów złośliwego oprogramowania lub umożliwiające jego instalację bądź dystrybucję;
- aplikacje lub kod innej firmy (np. SDK) zawierające komponent WebView z dodanym interfejsem JavaScript, który wczytuje niezaufane treści internetowe (np. adres URL HTTP) lub niezweryfikowane adresy URL uzyskane z niezaufanych źródeł (np. adresy URL z niezaufanych intencji).

Wprowadzanie w błąd

Zabraniamy publikowania aplikacji, które mogą wprowadzać użytkowników w błąd lub umożliwiać nieuczciwe postępowanie, w tym m.in. aplikacji, których działanie uznano za niemożliwe. Aplikacje muszą zawierać, opisywać i prezentować za pomocą zdjęć lub filmów swój sposób działania we wszystkich częściach metadanych. Nie mogą naśladować funkcji ani ostrzeżeń systemu operacyjnego lub innych aplikacji. Wszelkie zmiany w ustawieniach urządzenia muszą być wprowadzane za wiedzą i zgodą użytkownika. Powinny też dać się cofnąć.

Twierdzenia wprowadzające w błąd

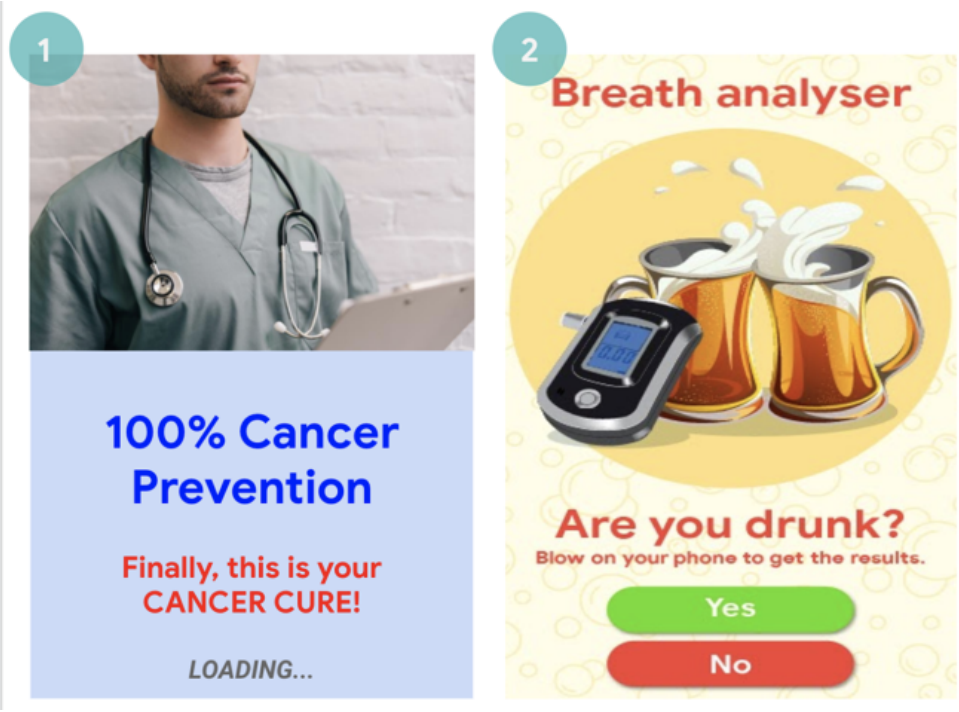
Zabraniamy publikowania aplikacji zawierających fałszywe lub mylące informacje między innymi w opisach, tytułach, ikonach i na zrzutach ekranu.

Aby zagwarantować, że platforma Google Play jest bezpiecznym i tolerancyjnym miejscem, stworzyliśmy standardy, które definiują i blokują materiały szkodliwe lub nieodpowiednie dla naszych użytkowników.

- Aplikacje z opisem niezgodnym z prawdą lub niedokładnym i niejasno przedstawiającym oferowane funkcje:

- aplikacja, której opis i zrzuty ekranu wskazują, że jest grą wyścigową (obraz przedstawiający samochód), a w rzeczywistości jest grą logiczną;
- aplikacja rzekomo będąca oprogramowaniem antywirusowym, ale zawierająca tylko poradnik dotyczący usuwania wirusów;

- aplikacje rzekomo zawierające funkcje, których zaimplementowanie jest niemożliwe (np. aplikacje odstraszające owady), nawet jeśli wyraźnie zaznaczono, że jest to żart czy dowcip;
- aplikacje, które są nieprawidłowo skategoryzowane, m.in. w zakresie oceny lub kategorii;
- treści w oczywisty sposób fałszywe lub wprowadzające w błąd, które mogą zakłócać procesy wyborcze;
- aplikacje, które niezgodnie z prawdą twierdzą, że są powiązane z organem państwowym lub umożliwiają załatwianie spraw urzędowych, choć nie mają wymaganych uprawnień;
- aplikacje sugerujące, że są oficjalnymi aplikacjami uznanego podmiotu (tytuły takie jak „Oficjalna aplikacja Justina Biebera" są niedozwolone, jeśli deweloper nie uzyskał potrzebnych pozwoleń lub praw).



(1) Ta aplikacja zawiera twierdzenia o charakterze medycznym lub zdrowotnym (lek na raka), które wprowadzają w błąd.
(2) Ta aplikacja zawiera funkcje, których zaimplementowanie jest niemożliwe (użycie telefonu jako alkomatu).

Zmiany ustawień urządzenia wprowadzające w błąd

Zabraniamy publikowania aplikacji wprowadzających zmiany poza samą aplikacją, w ustawieniach lub funkcjach urządzenia bez wiedzy i zgody użytkownika. Ustawienia i funkcje urządzenia to między innymi ustawienia systemowe i ustawienia przeglądarki, a także zakładki, skróty, ikony, widżety oraz informacje określające wyświetlanie aplikacji na ekranie głównym.

Dodatkowo nie są dozwolone:

- aplikacje modyfikujące ustawienia lub funkcje urządzenia za zgodą użytkownika, ale robiące to tak, że zmiany te trudno cofnąć;
- aplikacje lub reklamy zmieniające ustawienia lub funkcje urządzenia, by prowadziły do usług innych firm lub służyły do celów reklamowych;
- aplikacje podstępem doprowadzające użytkowników do usunięcia lub wyłączenia aplikacji innych firm lub zmiany ustawień urządzenia bądź funkcji;

- Aplikacje zachęcające lub nakłaniające użytkowników do usunięcia lub wyłączenia aplikacji innych firm lub do zmiany ustawień bądź funkcji urządzenia, chyba że dzieje się to w ramach możliwej do zweryfikowania usługi zabezpieczeń.

Umożliwianie nieuczciwego postępowania

Zabraniamy publikowania aplikacji, które ułatwiają użytkownikom wprowadzanie w błąd innych osób lub powodują jakiekolwiek działania wprowadzające w błąd, w tym między innymi aplikacji generujących lub ułatwiających generowanie dowodów osobistych, numerów ubezpieczenia społecznego, paszportów, dyplomów, kart kredytowych, kont bankowych czy praw jazdy. Aplikacje muszą prawidłowo ujawniać, tytułować, opisywać i prezentować za pomocą zdjęć lub filmów swój sposób działania lub swoją zawartość, a także działać w sposób, jakiego oczekuje użytkownik.

Dodatkowe zasoby aplikacji (na przykład zasoby gry) mogą być pobierane tylko wtedy, gdy są użytkownikowi niezbędne do korzystania z aplikacji. Pobrane zasoby muszą być zgodne ze wszystkimi zasadami Google Play. Przed rozpoczęciem pobierania aplikacja musi poprosić użytkownika o zgodę, jednoznacznie określając rozmiar pobieranego pliku.

Aplikacja musi przestrzegać naszych zasad, nawet jeśli powstała dla żartu lub w celach rozrywkowych (i podobnych).

Aby zagwarantować, że platforma Google Play jest bezpiecznym i tolerancyjnym miejscem, stworzyliśmy standardy, które definiują i blokują materiały szkodliwe lub nieodpowiednie dla naszych użytkowników.

- aplikacje, które udają inne aplikacje bądź witryny w celu nakłonienia użytkowników do ujawnienia danych osobowych lub uwierzytelniających;
- aplikacje przedstawiające niezweryfikowane lub prawdziwe numery telefonu, kontakty, adresy bądź informacje umożliwiające identyfikację osób lub podmiotów, które nie wyraziły zgody na wykorzystanie takich informacji;
- aplikacje, których najważniejsze funkcje różnią się w zależności od lokalizacji geograficznej użytkownika, parametrów urządzenia lub innych danych zależnych od użytkownika, a różnice te nie są wyraźnie widoczne na stronie z informacjami o aplikacji;
- aplikacje, które zmieniają się znacznie z wersji na wersję bez powiadamiania o tym użytkownika (np. w sekcji „Co nowego”) i aktualizowania strony z informacjami o aplikacji;
- aplikacje, które podczas sprawdzania próbują zmienić lub ukryć swoje zachowanie;
- aplikacje, którym sieć dystrybucji treści (CDN) umożliwia pobieranie plików bez pytania użytkownika o zgodę i informowania go o rozmiarze pliku przed rozpoczęciem pobierania.

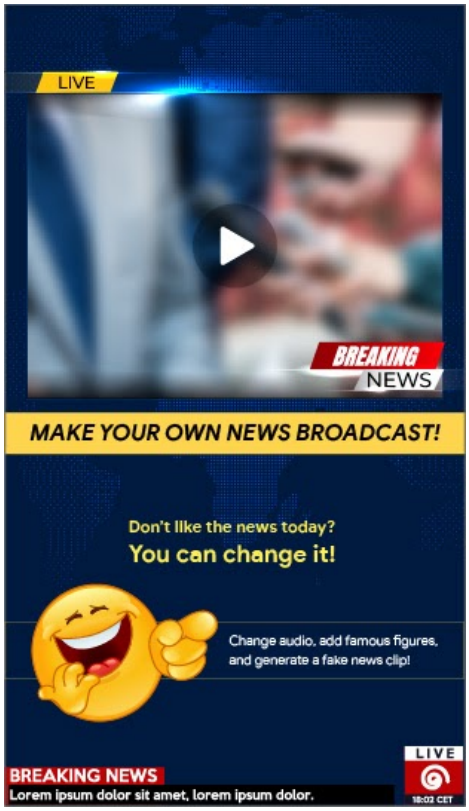
Zmanipulowane treści

Zabraniamy publikowania aplikacji, które promują lub tworzą fałszywe bądź wprowadzające w błąd informacje przy użyciu obrazów, filmów lub tekstu. Nie dopuszczamy aplikacji mających na celu promowanie lub podtrzymywanie niepodważalnie fałszywych lub wprowadzających w błąd obrazów, filmów bądź tekstów, które mogą powodować szkody, jeśli odnoszą się do napiętych wydarzeń, sytuacji politycznych, kwestii społecznych lub spraw istotnych z punktu widzenia zainteresowania publicznego.

Aplikacje, które modyfikują pliki multimedialne w zakresie wykraczającym poza typowe, akceptowalne z edytorskiego punktu widzenia poprawki ostrości lub jakości, muszą wyraźnie informować, że plik został zmieniony, lub dodawać do niego znak wodny w sytuacjach, gdy dla przeciętnego użytkownika mogłoby nie być oczywiste, że plik został zmieniony. Wyjątek może stanowić interes publiczny bądź oczywista satyra lub parodia.

Aby zagwarantować, że platforma Google Play jest bezpiecznym i tolerancyjnym miejscem, stworzyliśmy standardy, które definiują i blokują materiały szkodliwe lub nieodpowiednie dla naszych użytkowników.

- aplikacje umożliwiające dodanie osoby publicznej do demonstracji w okresie napiętej sytuacji politycznej;
- aplikacje wykorzystujące osoby publiczne lub pliki multimedialne związane z ważnymi wydarzeniami politycznymi do reklamowania na stronie z informacjami o aplikacji możliwości modyfikowania treści multimedialnych;
- aplikacje umożliwiające modyfikowanie klipów multimedialnych, tak by przypominały transmisję wiadomości.



(1) Ta aplikacja umożliwia modyfikowanie klipów multimedialnych, tak by przypominały transmisję wiadomości, oraz dodawanie znanych lub publicznych osób do klipu bez zamieszczenia znaku wodnego.

Przedstawianie nieprawdziwych informacji

Nie dopuszczamy aplikacji i kont dewelopera, które:

- podszywają się pod jakąkolwiek osobę lub organizację albo fałszywie identyfikują lub ukrywają swojego właściciela bądź główny cel;
- współdziałają, by wprowadzić użytkowników w błąd (dotyczy to m.in. aplikacji i kont deweloperów ukrywających lub fałszywie identyfikujących kraj, z którego pochodzą, a oferujących treści skierowane do użytkowników w innym kraju);
- współpracują z innymi aplikacjami, witrynami, deweloperami lub kontami, by ukrywać lub fałszywie identyfikować tożsamość dewelopera bądź aplikacji albo inne istotne szczegóły, jeśli zawartość aplikacji jest powiązana z polityką, kwestiami społecznymi lub sprawami istotnymi dla opinii publicznej.

Zasady dotyczące docelowego poziomu API w Google Play

Aby zapewnić użytkownikom bezpieczeństwo, w przypadku **wszystkich aplikacji** Google Play wymaga tych docelowych poziomów API:

Nowe aplikacje i aktualizacje aplikacji MUSZĄ być kierowane na poziom API Androida, który mieści się w przedziale roku od ostatniej głównej wersji Androida. Nowe aplikacje i aktualizacje, które nie spełnią tego wymogu, nie będą mogły być przesłane w Konsoli Play.

Aplikacje już dostępne w Google Play, które nie są aktualizowane i które nie są kierowane na poziom API mieszczący się w przedziale 2 lat od ostatniej głównej wersji Androida, nie będą dostępne dla nowych użytkowników, którzy mają na urządzeniach nowsze wersje systemu operacyjnego Android. Użytkownicy, którzy wcześniej zainstalowali taką aplikację z Google Play, nadal będą mogli ją znaleźć, ponownie zainstalować i używać na dowolnej wersji systemu operacyjnego Android obsługiwanej przez tę aplikację.

Porady techniczne na temat spełnienia wymogu docelowego poziomu API znajdziesz w przewodniku po migracji .

Dokładne terminy na zapewnienie zgodności znajdują się w tym artykule w Centrum pomocy .

Złośliwe oprogramowanie

Nasze zasady dotyczące złośliwego oprogramowania są proste: ekosystem Androida, łącznie ze Sklepem Google Play, oraz urządzenia użytkowników powinny być wolne od złośliwych działań (wykonywanych m.in. przez złośliwe oprogramowanie). Kierując się tą podstawową zasadą, staramy się zapewnić użytkownikom i ich urządzeniom z Androidem bezpieczny ekosystem.

Złośliwe oprogramowanie to każdy kod, który mógłby narazić na ryzyko użytkownika, jego dane lub urządzenie. Do tego typu oprogramowania zaliczamy między innymi potencjalnie szkodliwe aplikacje, pliki binarne i modyfikacje platformy, wśród których wyróżniamy kategorie takie jak konie trojańskie, phishing czy aplikacje szpiegowskie – lista tych kategorii jest cały czas aktualizowana.

Złośliwe oprogramowanie ma różne formy i możliwości, jednak zwykle jest tworzone w jednym z tych celów:

- naruszenie integralności urządzenia użytkownika;
- przejęcie kontroli nad urządzeniem użytkownika;
- umożliwienie osobie przeprowadzającej atak podejmowania zdalnych działań mających na celu uzyskanie dostępu do zainfekowanego urządzenia, używanie go lub eksploatowanie go w jakikolwiek inny sposób;
- wysłanie z urządzenia danych osobowych lub danych logowania bez wiedzy i zgody użytkownika;
- rozsyłanie spamu lub poleceń z zainfekowanych urządzeń na inne urządzenia lub do sieci;
- oszukanie użytkownika.

Aplikacje, pliki binarne lub modyfikacje platformy mogą być szkodliwe, tzn. mogą wykazywać złośliwe zachowania, nawet jeśli nie taka była intencja ich twórców. Dzieje się tak, ponieważ aplikacje, pliki binarne i modyfikacje platformy mogą działać inaczej w zależności od różnych zmiennych. Coś, co jednemu urządzeniu z Androidem szkodzi, dla innego może nie stanowić zagrożenia. Na przykład szkodliwe aplikacje, które wykorzystują do podejmowania złośliwych zachowań wycofane interfejsy API, nie zaszkodzą urządzeniu z najnowszą wersją Androida, jednak urządzenia z jego bardzo wczesną wersją mogą być narażone na ryzyko. Aplikacje, pliki binarne i modyfikacje platformy są oznaczane jako złośliwe oprogramowanie lub potencjalnie szkodliwe aplikacje, jeśli stwarzają wyraźne ryzyko dla niektórych lub wszystkich urządzeń z Androidem i ich użytkowników.

Poniższe kategorie złośliwego oprogramowania opracowaliśmy zgodnie z naszym głębokim przekonaniem, że użytkownicy powinni rozumieć, w jaki sposób ich urządzenia są wykorzystywane. Ułatwiają nam one tworzenie bezpiecznego ekosystemu, w którym możliwe jest wprowadzanie zdecydowanych innowacji i budowanie zaufania użytkowników.

Więcej informacji znajdziesz na stronie poświęconej Google Play Protect .

Tajny dostęp

Kod, który umożliwia przeprowadzenie na urządzeniu niechcianych, potencjalnie szkodliwych, kontrolowanych zdalnie operacji.

Mogą to być działania, których automatyczne wykonanie powodowałoby zaliczenie aplikacji, pliku binarnego lub modyfikacji platformy do jednej z kategorii złośliwego oprogramowania. Ogólnie rzecz biorąc, określenie „tajny dostęp" odnosi się do tego, w jaki sposób na urządzeniu może dojść do potencjalnie szkodliwych działań, dlatego nie można go do końca zakwalifikować do takich kategorii jak oszustwa związane z płatnościami czy komercyjne programy szpiegowskie. Z tego względu podkategoria tajnego dostępu jest czasem traktowana przez Google Play Protect jak luka w zabezpieczeniach.

Oszustwa obejmujące płatności

Kod, który wprowadza użytkownika w błąd i powoduje automatyczne naliczanie opłat.

Oszustwa obejmujące płatności mobilne dzielimy na fałszywe SMS-y, połączenia i dodatkowe opłaty.

Fałszywe SMS-y
Kod, który powoduje naliczanie opłat za wysyłanie płatnych SMS-ów bez pytania użytkownika o zgodę lub próbuje zamaskować aktywność związaną z obsługą wiadomości SMS przez ukrywanie umów albo powiadomień od operatora informujących użytkownika o pobieraniu opłat lub potwierdzających rozpoczęcie subskrypcji.

Czasami kod, technicznie rzecz biorąc, nie ukrywa wysyłania SMS-ów, ale wprowadza dodatkowe zachowania umożliwiające oszustwo. Przykłady obejmują ukrywanie fragmentów umowy przed użytkownikiem i blokowanie powiadomień SMS od operatora sieci komórkowej, które informują użytkownika o naliczaniu opłat lub rozpoczęciu subskrypcji.

Fałszywe połączenia
Kod, który powoduje naliczanie dodatkowych opłat za połączenia telefoniczne bez uzyskania zgody użytkownika.

Dodatkowe opłaty
Kod, który wprowadza użytkownika w błąd i powoduje dokonywanie niezamierzonych zakupów (w tym subskrypcji) przy użyciu rozliczeń przez operatora.

Takie oszustwa obejmują dowolny rodzaj opłat poza specjalnymi SMS-ami i połączeniami. Mogą to być płatności bezpośrednio u operatora, jak również opłaty za korzystanie z bezprzewodowych punktów dostępu czy transmisję danych. Najczęściej stosowane są opłaty za bezprzewodowe punkty dostępu. Użytkownik jest zwykle nakłaniany, by kliknął przycisk na dyskretnie wczytanym, przezroczystym komponencie WebView. Po wykonaniu takiej czynności rozpoczyna się uruchomienie cyklicznie odnawianej subskrypcji, a potwierdzający to SMS lub e-mail jest przechwytywany, by użytkownik nie zauważył transakcji.

Data wejścia w życie: 15 lutego 2023 r.

Stalkerware

Kod, który zbiera z urządzenia prywatne lub wrażliwe dane użytkownika i przesyła je osobom trzecim (firmom lub innym osobom) na potrzeby monitorowania.

Aplikacje muszą zawierać odpowiednie, dobrze widoczne informacje oraz uzyskać zgodę użytkowników. Opisaliśmy to w zasadach dotyczących danych użytkownika .

Wytyczne dla aplikacji monitorujących

Jedynymi dozwolonymi aplikacjami do monitorowania są te stworzone do monitorowania innych osób, np. do monitorowania dzieci przez rodziców, lub do zarządzania przedsiębiorstwem, np. do monitorowania poszczególnych pracowników, pod warunkiem że spełniają one wszystkie wymagania opisane poniżej. Aplikacje takie nie mogą być używane do śledzenia nikogo innego (np. współmałżonka), nawet za zgodą i wiedzą tej osoby oraz nawet przy wyświetlanym stałym

powiadomieniu. Te aplikacje muszą wykorzystywać w pliku manifestu flagę metadanych IsMonitoringTool, aby prawidłowo oznaczać się jako aplikacje monitorujące.

Aplikacje monitorujące muszą spełniać te wymagania:

- Aplikacje nie mogą prezentować się jako rozwiązania służące do szpiegowania lub podglądania.
- Aplikacje nie mogą ukrywać ani maskować monitorowania ani próbować wprowadzać użytkowników w błąd co do działania takich funkcji.
- Aplikacje muszą wyświetlać użytkownikom stałe powiadomienie przez cały czas działania oraz unikalną ikonę jasno określającą aplikację.
- Aplikacje muszą ujawniać funkcję monitorowania lub śledzenia w opisie w Sklepie Google Play.
- Aplikacje i informacje o aplikacjach w Google Play nie mogą w żaden sposób umożliwiać aktywowania ani użycia funkcji, które naruszają nasze warunki, np. nie mogą zawierać linków do niezgodnego pakietu APK spoza Google Play.
- Aplikacje muszą być zgodne z obowiązującymi przepisami prawa. Ponosisz pełną odpowiedzialność za to, aby Twoja aplikacja była zgodna z przepisami docelowego kraju lub regionu.

Atak typu DoS

Kod, który bez wiedzy użytkownika wykonuje atak typu DoS lub jest częścią rozproszonego ataku typu DoS kierowanego na inne systemy i zasoby.

Może to na przykład polegać na masowym wysyłaniu żądań HTTP w celu wygenerowania nadmiernego obciążenia zdalnych serwerów.

Szkodliwe programy pobierające

Kod, który sam w sobie nie jest groźny, ale pobiera inne potencjalnie szkodliwe aplikacje.

Kod może być uznany za służący do pobierania szkodliwych elementów w tych przypadkach:

- Istnieje podejrzenie, że kod został utworzony do pobierania potencjalnie szkodliwych aplikacji, pobrał takie aplikacje lub zawiera kod, który może pobierać i instalować aplikacje.
- Co najmniej 5% aplikacji pobranych przez ten kod to potencjalnie szkodliwe aplikacje. Minimalny próg wyliczeń to 500 zarejestrowanych pobrań aplikacji (25 zarejestrowanych pobrań potencjalnie szkodliwych aplikacji).

Główne przeglądarki i aplikacje do udostępniania plików nie są uznawane za szkodliwe programy pobierające, jeśli spełniają te warunki:

- Nie pobierają plików bez interakcji użytkownika.
- Wszystkie pobrania potencjalnie szkodliwych aplikacji są uruchomione przez użytkowników wyrażających na to zgodę.

Zagrożenie, które nie obejmuje Androida

Kod zawierający zagrożenia, które nie dotyczą Androida.

Takie aplikacje nie są zagrożeniem dla użytkownika urządzenia z Androidem ani samego urządzenia z tym systemem, ale zawierają komponenty, które mogą być szkodliwe na innych platformach.

Phishing

Kod, który stwarza pozory, że pochodzi z zaufanego źródła, żądający danych uwierzytelniających lub rozliczeniowych użytkownika w celu wysłania ich do osoby trzeciej. Ta kategoria obejmuje również kod, który przechwytuje dane logowania użytkownika podczas ich przesyłania.

Częstym celem ataków phishingowych są dane logowania do banku, numery kart kredytowych i dane logowania do kont internetowych w sieciach społecznościowych lub grach.

Nadużywanie eskalowanych uprawnień

Kod, który narusza integralność systemu poprzez uszkodzenie piaskownicy aplikacji, zdobycie podwyższonych uprawnień albo zmianę lub wyłączenie dostępu do podstawowych funkcji związanych z bezpieczeństwem.

Przykłady:

- Aplikacja, która nie jest zgodna z modelem uprawnień Androida lub wykrada dane logowania (na przykład tokeny OAuth) z innych aplikacji.
- Aplikacje, które nadużywają różnych funkcji, by uniemożliwić ich odinstalowanie lub zatrzymanie.
- Aplikacja, która wyłącza SELinux.

Aplikacje eskalujące uprawnienia, które umożliwiają dostęp do roota urządzenia bez pytania użytkownika o zgodę, są klasyfikowane jako aplikacje umożliwiające dostęp do roota.

Ransomware

Kod, który częściowo lub w znacznym stopniu przejmuje kontrolę nad urządzeniem bądź danymi na urządzeniu i żąda od użytkownika płatności lub wykonania jakiejś czynności w zamian za zwrócenie kontroli.

Niektóre programy typu ransomware szyfrują dane na urządzeniu i żądają płatności w zamian za ich odszyfrowanie lub wykorzystują funkcje administracyjne urządzenia, by typowy użytkownik nie był w stanie ich usunąć. Przykłady:

- Uniemożliwienie użytkownikowi dostępu do urządzenia i żądanie pieniędzy w zamian za zwrócenie kontroli.
- Szyfrowanie danych na urządzeniu i żądanie zapłaty, po której rzekomo ma nastąpić odszyfrowanie.
- Wykorzystywanie funkcji menedżera zasad urządzenia w celu uniemożliwienia użytkownikowi usunięcia aplikacji.

Kod rozpowszechniany razem z urządzeniem, którego głównym celem jest finansowanie zarządzania urządzeniem, może być wykluczony z kategorii ransomware, jeśli spełni wymagania dotyczące bezpiecznego blokowania i zarządzania oraz odpowiedniego informowania użytkownika i uzyskiwania jego zgody.

Dostęp do roota

Kod, który ma dostęp do roota na urządzeniu.

Kod umożliwiający dostęp do roota może być nieszkodliwy lub szkodliwy. Nieszkodliwe aplikacje z dostępem do roota powiadamiają użytkownika o zamiarze uzyskania dostępu do roota – nie wykonują groźnych działań, które są charakterystyczne dla innych potencjalnie szkodliwych aplikacji.

Złośliwe aplikacje z dostępem do roota nie informują użytkownika o zamiarze uzyskania takiego dostępu albo powiadamiają o tym użytkownika, ale wykonują też inne działania, które kwalifikują je jako potencjalnie szkodliwe aplikacje.

Spam

Kod, który wysyła niechciane wiadomości do kontaktów użytkownika lub wykorzystuje urządzenie jako narzędzie do wysyłania spamerskich e-maili.

Programy szpiegowskie

Kod, który przekazuje dane osobowe z urządzenia bez wiedzy i zgody użytkownika.

Za działanie programu szpiegowskiego można uznać na przykład przekazywanie którychkolwiek z poniższych danych bez ujawniania tego faktu użytkownikowi lub w sposób, którego użytkownik się

nie spodziewa:

- lista kontaktów,
- zdjęcia lub inne pliki pochodzące z karty SD bądź nienależące do aplikacji,
- treści z konta e-mail użytkownika,
- rejestr połączeń,
- rejestr SMS-ów,
- historia online lub zakładki z domyślnej przeglądarki,
- informacje z katalogów /data/ innych aplikacji.

Działania, które mogą uchodzić za szpiegowanie użytkownika, mogą też zostać oznaczone jako działanie programu szpiegowskiego. Jako przykład takich działań można podać nagrywanie dźwięku lub połączeń telefonicznych albo wykradanie danych aplikacji.

Koń trojański

Kod, który stwarza wrażenie niegroźnego (np. gra rzekomo będąca zwykłą grą), ale w rzeczywistości wykonuje niepożądane działania skierowane przeciwko użytkownikowi.

Tej klasyfikacji używa się zwykle w połączeniu z innymi kategoriami potencjalnie szkodliwych aplikacji. Koń trojański zawiera element nieszkodliwy oraz ukryty komponent szkodliwy. Może to być na przykład gra, która bez zgody użytkownika wysyła w tle specjalne SMS-y z urządzenia.

Uwaga na temat nietypowych aplikacji

Nowe lub rzadkie aplikacje mogą zostać uznane za nietypowe, jeśli Google Play Protect nie ma dość informacji, by zagwarantować, że są bezpieczne. Nie znaczy to, że aplikacja jest na pewno szkodliwa, jednak bez dalszej weryfikacji nie można tego wykluczyć.

Uwaga dotycząca kategorii „tajny dostęp”

Zaliczenie złośliwego oprogramowania do kategorii „tajny dostęp” zależy od zachowania, jakie wykazuje kod. Warunkiem koniecznym do zaliczenia kodu do tej kategorii jest umożliwianie przez niego działań, których automatyczne wykonanie mogłoby powodować zaliczenie tego kodu do jednej z innych kategorii złośliwego oprogramowania. Za złośliwe oprogramowanie typu „tajny dostęp” można na przykład uznać aplikację umożliwiającą dynamiczne ładowanie kodu, który następnie zacznie wyodrębniać SMS-y.

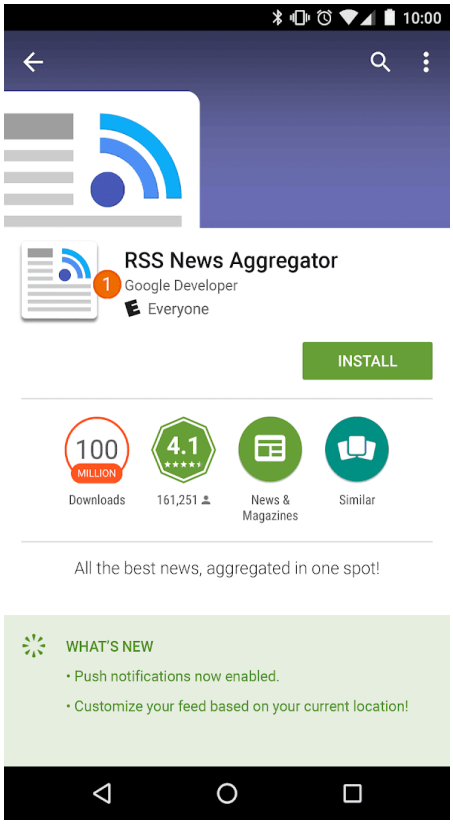
Jeśli jednak aplikacja umożliwia wykonanie dowolnego kodu, ale nie mamy podstaw, by sądzić, że jego wykonanie zostało dodane w celu podjęcia złośliwych działań, nie uznamy tej aplikacji za złośliwe oprogramowanie typu „tajny dostęp”, a jedynie stwierdzimy, że ma ona luki w zabezpieczeniach, i poprosimy dewelopera o wprowadzenie poprawki.

Podszywanie się pod inne osoby

Zabraniamy publikowania aplikacji, które wprowadzają użytkowników w błąd, podszywając się pod inną osobę (np. innego dewelopera, firmę, podmiot) lub inną aplikację. Nie sugeruj, że Twoja aplikacja jest z kimś powiązana lub przez kogoś autoryzowana, jeśli tak nie jest. Uważaj, by nie używać ikon, opisów, tytułów ani elementów aplikacji, które mogą wprowadzać użytkowników w błąd co do relacji między Twoją aplikacją a inną osobą lub aplikacją.

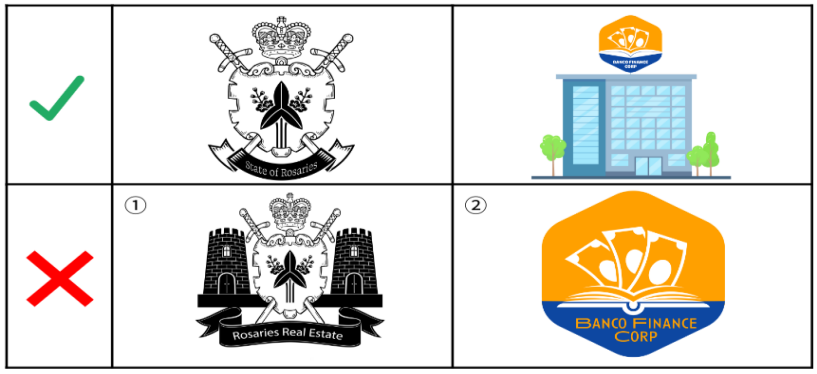
Aby zagwarantować, że platforma Google Play jest bezpiecznym i tolerancyjnym miejscem, stworzyliśmy standardy, które definiują i blokują materiały szkodliwe lub nieodpowiednie dla naszych użytkowników.

- Deweloperzy fałszywie sugerujący powiązania z inną firmą/organizacją lub innym deweloperem/podmiotem.



① Wyświetlana nazwa dewelopera tej aplikacji sugeruje, że jest on oficjalnie powiązany z Google, co nie jest prawdą.

- Aplikacje, których ikony i tytuły fałszywie sugerują powiązania z inną firmą/organizacją lub innym deweloperem/podmiotem.



① Aplikacja używa godła państwowego, czym wprowadza użytkowników w błędne przekonanie, że jest powiązana z organami administracji państwowej.
②Aplikacja wykorzystuje logo firmy, które sugeruje, że jest to aplikacja tej firmy, co nie jest prawdą.

- Tytuły i ikony aplikacji bardzo podobne do tych, które są znane z istniejących już produktów lub usług, co może wprowadzać użytkowników w błąd.

① Aplikacja ma w ikonie logo popularnej strony związanej z kryptowalutami, co sugeruje, że jest to oficjalna aplikacja tej strony.
② Ikona aplikacji przedstawia bohatera i tytuł popularnego serialu, sugerując użytkownikom, że jest jego podmiotem stowarzyszonym, co nie jest prawdą.

- Aplikacje sugerujące, że są oficjalnymi aplikacjami uznanego podmiotu. Tytuły takie jak „Oficjalna aplikacja Justina Biebera” nie są dozwolone, jeśli deweloper nie uzyskał potrzebnych pozwoleń lub praw.
- Aplikacje naruszające wskazówki dotyczące marki Android .

Mobile Unwanted Software

W Google uważamy, że jeśli skoncentrujemy się na użytkowniku, reszta przyjdzie sama. W naszych zasadach dotyczących oprogramowania i zasadach dotyczących niechcianego oprogramowania podajemy ogólne zalecenia dotyczące oprogramowania, które zapewnia użytkownikom pozytywne wrażenia. Ta zasada uzupełnia nasze zasady dotyczące niechcianego oprogramowania – określa wytyczne dotyczące ekosystemu Androida i Sklepu Google Play. Oprogramowanie naruszające te zasady może być szkodliwe, dlatego staramy się chronić przed nim użytkowników.

Jak wspominamy w zasadach dotyczących niechcianego oprogramowania, odkryliśmy, że większość oprogramowania tego typu ma co najmniej 1 z tych cech:

- wprowadza w błąd, obiecując korzyści, których w rzeczywistości nie przynosi;
- próbuje nakłonić użytkownika do instalacji lub instaluje się razem z innym programem;
- nie informuje użytkownika o swoich głównych lub istotnych funkcjach;
- w nieoczekiwany sposób wpływa na system użytkownika;
- gromadzi lub przesyła prywatne informacje bez wiedzy użytkownika;
- gromadzi lub przesyła prywatne informacje, nie zabezpieczając ich (np. za pomocą HTTPS);
- jest w pakiecie z innym oprogramowaniem, a jego obecność nie jest ujawniana.

Na urządzeniach mobilnych oprogramowanie to kod w formie aplikacji, pliku binarnego, modyfikacji platformy itp. Nie dopuszczamy oprogramowania szkodliwego dla ekosystemu programów lub

zaburzającego wygodę użytkownika, dlatego będziemy podejmować działania wobec kodu, który narusza te zasady.

Poniżej zamieszczamy uzupełnienie zasad dotyczących niechcianego oprogramowania, które rozszerza ich zastosowanie na aplikacje mobilne. Razem z tymi zasadami będziemy dopracowywać też zasady dotyczące niechcianych aplikacji mobilnych, uwzględniając kolejne rodzaje nadużyć.

Przejrzyste zachowanie i jednoznaczne informacje

Cały kod powinien być zgodny z tym, co deweloper obiecał użytkownikom. Aplikacje powinny mieć wszystkie opisywane funkcje. Aplikacje nie mogą wprowadzać użytkowników w błąd.

- Aplikacje powinny mieć jasno określone funkcje i cele.
- Jasno i wyraźnie wyjaśnij użytkownikowi, jakie zmiany w systemie wprowadzi aplikacja. Pozwól użytkownikom przejrzeć i zaakceptować wszystkie istotne opcje instalacji i zmiany.
- Oprogramowanie nie może błędnie przedstawiać użytkownikowi stanu jego urządzenia, na przykład twierdząc, że system jest w stanie krytycznym lub został zainfekowany wirusami.
- Nie używaj nieprawidłowej aktywności, by zwiększyć ruch z reklam lub liczbę konwersji.
- Zabraniamy publikowania aplikacji, które wprowadzają użytkowników w błąd, podszywając się pod inną osobę (np. innego dewelopera, firmę, podmiot) lub inną aplikację. Nie sugeruj, że Twoja aplikacja jest z kimś powiązana lub przez kogoś autoryzowana, jeśli tak nie jest.

Przykłady naruszenia zasad:

- oszustwo reklamowe,
- inżynieria społeczna.

Ochrona danych użytkownika

Jasno i zrozumiale informuj użytkowników o dostępie do danych osobowych i poufnych oraz ich używaniu i udostępnianiu. Wykorzystując dane użytkownika, musisz przestrzegać wszystkich obowiązujących zasad dotyczących danych użytkownika i podejmować odpowiednie środki, by te dane chronić.

- Daj użytkownikom możliwość wyrażenia zgody na zbieranie ich danych, zanim zaczniesz te dane zbierać i wysyłać z urządzenia. Dotyczy to danych o kontach osób trzecich, adresach e-mail, numerach telefonów, zainstalowanych aplikacjach, plikach, lokalizacji oraz wszelkich innych danych osobowych i poufnych, których zbierania użytkownik się nie spodziewał.
- Ze wszystkimi danymi osobowymi i poufnymi użytkownika postępuj w bezpieczny sposób, używając nowoczesnych metod szyfrowania (np. protokołu HTTPS).
- Oprogramowanie, w tym aplikacje mobilne, może przesyłać na serwery tylko te dane osobowe i poufne użytkowników, które są powiązane z działaniem aplikacji.

Przykłady naruszenia zasad:

- zbieranie danych (program szpiegowski),
- nadużycie uprawnień z ograniczeniami.

Przykładowe zasady dotyczące danych użytkownika:

- *Zasady dotyczące danych użytkownika w Google Play*
- *Wymagania GMS dotyczące danych użytkownika*
- *Zasady usług interfejsu API Google dotyczące danych użytkownika*

Niezakłócanie działania urządzeń mobilnych

Obsługa aplikacji powinna być prosta, zrozumiała i oparta na jednoznacznych wyborach użytkownika. Aplikacja powinna przedstawiać użytkownikowi wyraźną propozycję wartości, a jej reklamowane lub oczekiwane działanie nie powinno być zakłócane.

- Nie wyświetlaj reklam, które pojawiają się w nieoczekiwany sposób, np. zakłócając lub utrudniając korzystanie z funkcji urządzenia, albo pokazują się poza środowiskiem aplikacji i nie mają możliwości łatwego zamknięcia, zaakceptowania czy atrybucji.
- Aplikacje nie mogą zakłócać działania urządzenia ani innych aplikacji.
- Proces odinstalowania (jeśli jest możliwy) powinien być jasny i zrozumiały.
- Aplikacje mobilne nie mogą wyświetlać komunikatów przypominających te z systemu operacyjnego urządzenia lub innych aplikacji. Nie ukrywaj przed użytkownikiem alertów z innych aplikacji lub systemu operacyjnego, szczególnie tych informujących użytkownika o zmianach w systemie operacyjnym.

Przykłady naruszenia zasad:

- uciążliwe reklamy,
- nieautoryzowane używanie funkcji systemowych lub podszywanie się pod nie.

Szkodliwe programy pobierające

Kod, który sam w sobie nie jest niechcianym oprogramowaniem, ale pobiera inne niechciane oprogramowanie mobilne.

Kod może być uznany za służący do pobierania szkodliwych elementów w tych przypadkach:

- Istnieje podejrzenie, że kod został utworzony do pobierania niechcianego oprogramowania mobilnego, pobrał takie oprogramowanie lub zawiera kod, który może pobierać i instalować aplikacje.
- Co najmniej 5% aplikacji pobranych przez ten kod to niechciane oprogramowanie mobilne. Minimalny próg wyliczeń to 500 zarejestrowanych pobrań aplikacji (25 zarejestrowanych pobrań niechcianego oprogramowania mobilnego).

Główne przeglądarki i aplikacje do udostępniania plików nie są uznawane za szkodliwe programy pobierające, jeśli spełniają te warunki:

- Nie pobierają one plików bez interakcji użytkownika.
- Wszystkie pobrania aplikacji są uruchomione przez użytkowników wyrażających na to zgodę.

Oszustwo reklamowe

Oszustwa reklamowe są surowo zabronione. Interakcje z reklamami generowane w celu przekonania sieci reklamowej, że ruch jest efektem autentycznego zainteresowania użytkownika, to oszustwo reklamowe, które jest formą nieprawidłowego ruchu. Oszustwa reklamowe mogą być efektem ubocznym działań deweloperów, którzy implementują reklamy w niedozwolony sposób, np. wyświetlają ukryte lub klikane automatycznie reklamy, modyfikują informacje albo w inny sposób wykorzystują działania automatyczne (roboty, boty itp.) lub wykonywane przez ludzi, które mają na celu wygenerowanie nieprawidłowego ruchu z reklam. Nieprawidłowy ruch i oszustwa reklamowe są szkodliwe dla reklamodawców, deweloperów i użytkowników oraz prowadzą do utraty zaufania do ekosystemu reklam mobilnych.

Aby zagwarantować, że platforma Google Play jest bezpiecznym i tolerancyjnym miejscem, stworzyliśmy standardy, które definiują i blokują materiały szkodliwe lub nieodpowiednie dla naszych użytkowników.

- aplikacja, która renderuje reklamy niewidoczne dla użytkownika;
- aplikacja, która automatycznie generuje niezamierzone przez użytkownika kliknięcia reklam albo generuje ruch w sieci pochodzący z fałszywego przypisywania kliknięć;
- aplikacja wysyłająca fałszywe informacje o atrybucji kliknięć przycisku instalacji, by otrzymać zapłatę za instalacje, które nie pochodzą z sieci nadawcy;

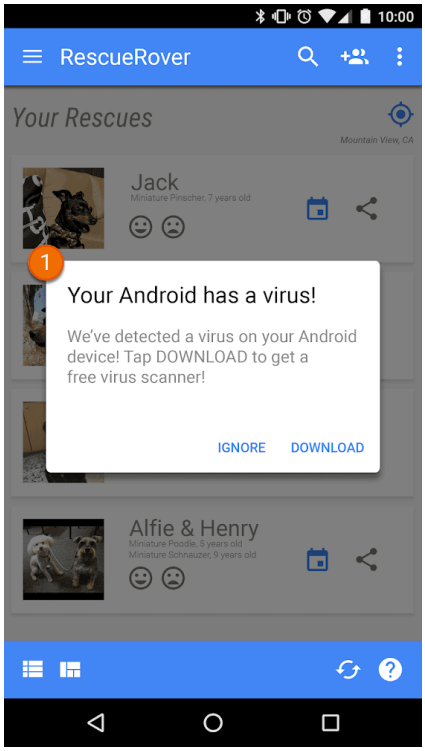
- aplikacja, która wyświetla wyskakujące reklamy, gdy użytkownik nie korzysta z jej interfejsu;
- aplikacja podająca fałszywe informacje o zasobach reklamowych, np. aplikacja informująca sieci reklamowe, że działa na urządzeniu z iOS, podczas gdy w rzeczywistości działa na urządzeniu z Androidem, albo aplikacja, która podaje nieprawdziwą nazwę pakietu, na którym zarabia deweloper.

Nieautoryzowane używanie funkcji systemowych lub podszywanie się pod nie

Niedozwolone są aplikacje i reklamy, które naśladują lub zakłócają funkcje systemowe, np. powiadomienia i ostrzeżenia. Powiadomienia na poziomie systemu mogą być używane tylko przez integralne funkcje aplikacji (np. aplikacja linii lotniczej może informować użytkowników o ofertach specjalnych, a gra powiadamiać o dostępnych w niej promocjach).

Aby zagwarantować, że platforma Google Play jest bezpiecznym i tolerancyjnym miejscem, stworzyliśmy standardy, które definiują i blokują materiały szkodliwe lub nieodpowiednie dla naszych użytkowników.

- Aplikacje lub reklamy dostarczane przy użyciu powiadomienia lub alertu systemowego:



① Powiadomienie systemowe pokazane w tej aplikacji jest używane do wyświetlenia reklamy.

Więcej przykładów tego typu znajdziesz w zasadach dotyczących reklam.

Social Engineering

We do not allow apps that pretend to be another app with the intention of deceiving users into performing actions that the user intended for the original trusted app.

Zabronione jest publikowanie aplikacji z reklamami, które są uciążliwe lub zawierają treści wprowadzające w błąd. Reklamy mogą wyświetlać się tylko w aplikacji, która je zawiera. Reklamy

wyświetlane w aplikacji traktujemy jako część aplikacji. Muszą one być zgodne ze wszystkimi naszymi zasadami. Zasady dotyczące reklam związanych z hazardem znajdziesz tutaj.

Google Play umożliwia stosowanie wielu strategii generowania przychodów, w tym dystrybucji płatnej i sprzedaży produktów w aplikacji, a także subskrypcji oraz modeli opartych na reklamach. Strategie te są korzystne zarówno dla deweloperów, jak i użytkowników. Dbając o wygodę użytkowników, wymagamy od deweloperów przestrzegania naszych zasad.

Płatności

1. Deweloperzy, którzy naliczają opłaty za aplikacje pobierane z Google Play, jako formy płatności za te transakcje muszą używać systemu rozliczeniowego Google Play.
2. Aplikacje dostępne w Google Play, które wymagają lub akceptują płatności za dostęp do funkcji lub usług w samej aplikacji, w tym dostęp do funkcji, treści cyfrowych lub towarów (łącznie „zakupy w aplikacji"), jako formy płatności za te transakcje muszą używać systemu rozliczeniowego Google Play, chyba że zastosowanie ma artykuł 3 lub 8.

   Oto przykłady funkcji lub usług dostępnych w ramach zakupów w aplikacji i wymagających korzystania z systemu rozliczeniowego Google Play:

   - elementy (takie jak wirtualne waluty, dodatkowe życia, dodatkowy czas gry, przedmioty, postacie czy awatary);
   - usługi wymagające subskrypcji (np. usługi do fitnessu czy gier, a także usługi randkowe, edukacyjne, muzyczne, filmowe czy lepsze wersje dotychczasowych usług);
   - funkcje lub treści w aplikacji (np. aplikacja w wersji bez reklam czy nowe funkcje niedostępne w jej bezpłatnej wersji);
   - oprogramowanie i usługi działające w chmurze (w tym usługi przechowywania danych, oprogramowanie biznesowe czy programy do zarządzania finansami).

3. Systemu rozliczeniowego Google Play nie można używać, jeśli:
   a. płatność dotyczy głównie:
      - zakupu lub wypożyczenia towarów fizycznych (takich jak artykuły spożywcze, ubrania, artykuły gospodarstwa domowego, elektronika);
      - zakupu usług fizycznych (takich jak transport, sprzątanie, loty, karnety na siłownię, dostawa jedzenia, bilety na wydarzenia);
      - przelewu powiązanego z rachunkiem karty kredytowej lub rachunkiem za media (np. za telewizję kablową lub usługi telekomunikacyjne);

   b. płatności peer-to-peer, aukcji online lub darowizn zwolnionych z podatku;
   c. płatności za treści lub usługi umożliwiające hazard online, zgodnie z opisem w sekcji Aplikacje hazardowe w zasadach dotyczących hazardu, gier i konkursów na pieniądze;
   d. dowolnej kategorii produktów uznanej za niedopuszczalną zgodnie z polityką treści Centrum płatności.

   Uwaga: na niektórych rynkach na potrzeby aplikacji sprzedających fizyczne towary lub usługi oferujemy usługę Google Pay. Więcej informacji znajdziesz na stronie Google Pay dla deweloperów.

4. Z wyjątkiem sytuacji opisanych w artykule 3 i 8, aplikacje nie mogą kierować użytkowników do form płatności innych niż system rozliczeniowy Google Play. Zakaz ten obejmuje między innymi kierowanie użytkowników do innych form płatności za pomocą:
   - informacji o aplikacji w Google Play;
   - promocji w aplikacji związanych z treściami, które można kupić;
   - komponentów WebView, przycisków, linków, komunikatów, reklam lub innych form wezwania do działania;

- procesów realizowanych w interfejsie aplikacji, w tym procesu tworzenia konta lub rejestracji, które kierują użytkowników z aplikacji do formy płatności innej niż system rozliczeniowy Google Play.

5. Wirtualnej waluty można używać tylko w aplikacji lub grze, w której została ona kupiona.
6. Deweloperzy muszą jasno i precyzyjnie informować użytkowników o warunkach i cenach swoich aplikacji oraz wszelkich oferowanych w nich funkcjach i subskrypcjach. Ceny w aplikacji muszą odpowiadać cenom wyświetlanym w interfejsie Płatności w Play. Jeśli opis produktu w Google Play dotyczy funkcji w aplikacji podlegających określonym lub dodatkowym opłatom, strona z opisem aplikacji musi zawierać wyraźną informację, że dostęp do tych funkcji jest płatny.
7. Aplikacje i gry z mechanizmem otrzymywania losowych wirtualnych produktów po zakupie, w tym między innymi „skrzynek z łupami", muszą wyraźnie prezentować informacje o szansie otrzymania takich produktów bezpośrednio przed dokonaniem zakupu.
8. O ile nie występują okoliczności opisane w artykule 3, deweloperzy udostępniający w Google Play swoje aplikacje, które są przeznaczone na telefony oraz tablety i które wymagają lub akceptują płatności od użytkowników z Korei Południowej w zamian za dostęp do zakupów w aplikacji, w przypadku tych transakcji mogą też oferować rozliczenia w samej aplikacji oprócz korzystania z systemu rozliczeniowego Google Play. Deweloperzy, którzy chcą oferować tę funkcję, powinni wypełnić formularz deklaracji dodatkowego systemu rozliczeń w aplikacji i wyrazić zgodę na zawarte w nim dodatkowe warunki i wymagania programu.

Uwaga: jeśli chcesz zobaczyć terminy wejścia w życie tych zasad i najczęstsze pytania na ich temat, odwiedź nasze Centrum pomocy.

Zabronione jest publikowanie aplikacji z reklamami, które są uciążliwe lub zawierają treści wprowadzające w błąd. Reklamy mogą wyświetlać się tylko w aplikacji, która je zawiera. Reklamy wyświetlane w aplikacji traktujemy jako część aplikacji. Muszą one być zgodne ze wszystkimi naszymi zasadami. Zasady dotyczące reklam związanych z hazardem znajdziesz tutaj.

Zabraniamy publikowania aplikacji z reklamami, które są uciążliwe lub zawierają treści wprowadzające w błąd. Reklamy mogą wyświetlać się tylko w aplikacji, która je zawiera. Reklamy oraz powiązane z nimi oferty wyświetlane w Twojej aplikacji są przez nas uważane za część tej aplikacji. Reklamy widoczne w Twojej aplikacji muszą być zgodne ze wszystkimi naszymi zasadami. Zasady dotyczące reklam związanych z hazardem znajdziesz tutaj .

Użycie danych o lokalizacji do wyświetlania reklam

Aplikacje, w których korzystanie z danych o lokalizacji urządzenia za pozwoleniem użytkownika zostaje poszerzone o wyświetlanie reklam, muszą być zgodne z zasadami opisanymi w sekcji Dane osobowe i poufne oraz dodatkowo z tymi wymaganiami:

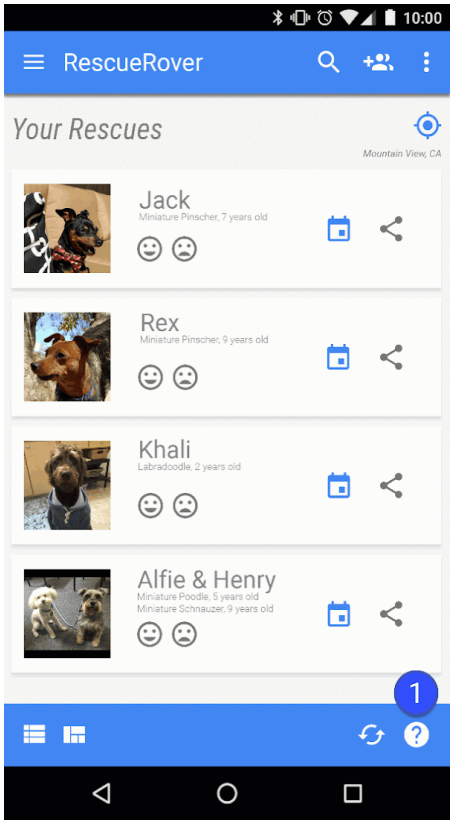
- Używanie lub zbieranie danych o lokalizacji urządzenia za pozwoleniem użytkownika do celów reklamowych musi być jasne dla użytkownika i udokumentowane w obowiązkowej polityce prywatności aplikacji. Obejmuje to podanie linków do polityki prywatności poszczególnych sieci reklamowych, w których są opisane zasady użycia danych o lokalizacji.
- Zgodnie z wymaganiami dostępu do lokalizacji aplikacja może o niego prosić tylko w celu zastosowania bieżących funkcji lub usług oraz nie może o niego prosić wyłącznie na potrzeby wyświetlania reklam.

Reklamy wprowadzające w błąd

Reklamy nie mogą symulować ani udawać interfejsu żadnej aplikacji ani powiadomień i ostrzeżeń systemowych. W przypadku każdej reklamy użytkownik musi dokładnie wiedzieć, jaka aplikacja ją wyświetla.

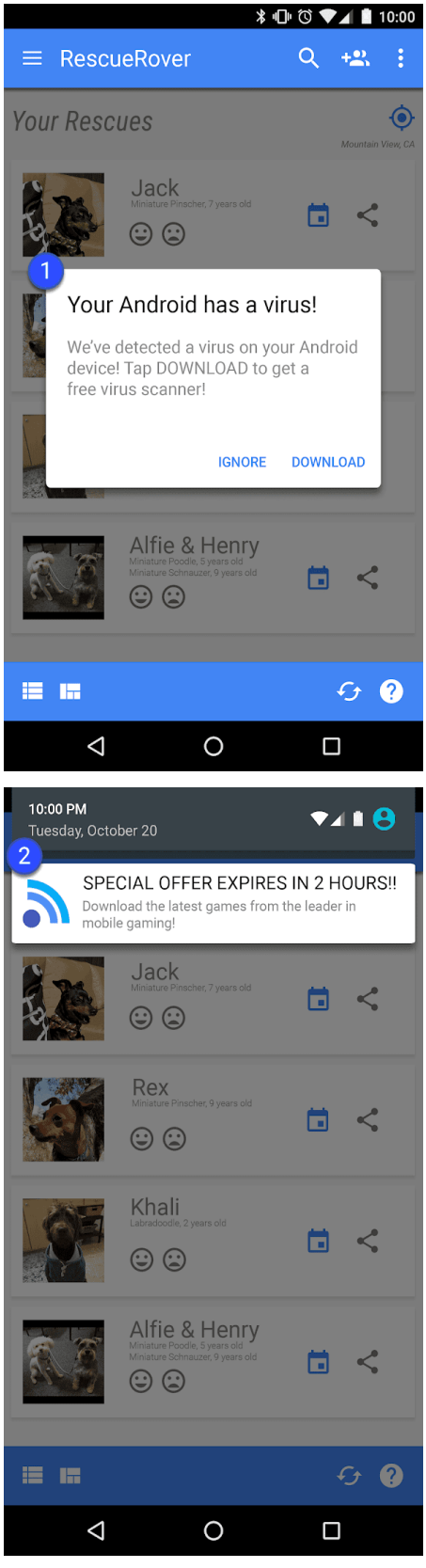
Aby zagwarantować, że platforma Google Play jest bezpiecznym i tolerancyjnym miejscem, stworzyliśmy standardy, które definiują i blokują materiały szkodliwe lub nieodpowiednie dla naszych użytkowników.

- Reklamy udające interfejs aplikacji.



① Ikona znaku zapytania w tej aplikacji to reklama, która powoduje otwarcie zewnętrznej strony docelowej.

- Reklamy udające powiadomienia systemowe.



① ② Te reklamy udają różne powiadomienia systemowe.

Zarabianie na ekranie blokady

Jeśli jedynym celem aplikacji nie jest blokowanie ekranu, nie może ona wprowadzać na zablokowanym ekranie urządzenia reklam ani funkcji umożliwiających deweloperowi zarabianie.

Uciążliwe reklamy

Uciążliwe reklamy to reklamy wyświetlane użytkownikom w nieoczekiwany sposób, co może skutkować niezamierzonymi kliknięciami lub zakłócać działanie funkcji urządzenia.

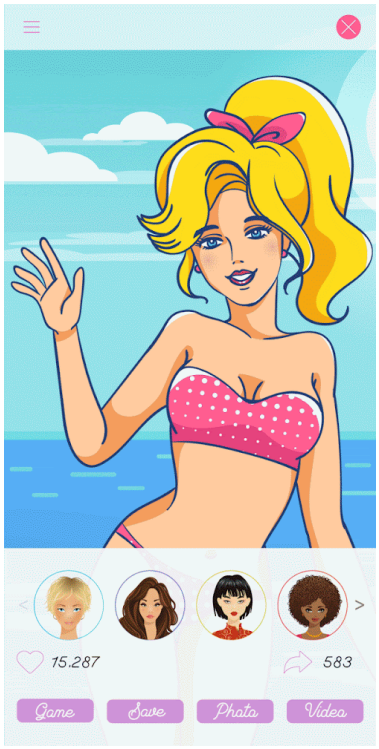
Zmuszanie użytkownika do kliknięcia reklamy lub przesłania danych osobowych w celach marketingowych, zanim może on w pełni korzystać z aplikacji, jest zabronione. Reklamy pełnoekranowe mogą wyświetlać się wyłącznie w aplikacji, która je zawiera. Jeśli aplikacja wyświetla reklamy pełnoekranowe lub inne reklamy, które zakłócają jej normalne działanie, użytkownik musi mieć możliwość ich łatwego zamknięcia bez żadnych negatywnych konsekwencji.

Aby zagwarantować, że platforma Google Play jest bezpiecznym i tolerancyjnym miejscem, stworzyliśmy standardy, które definiują i blokują materiały szkodliwe lub nieodpowiednie dla naszych użytkowników.

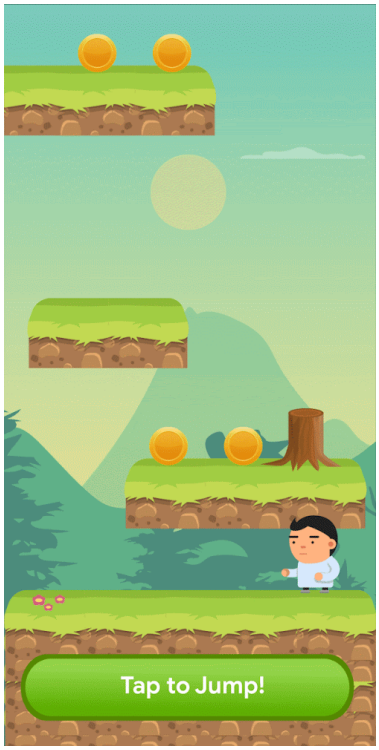
- Reklamy zajmujące pełny ekran lub zakłócające normalne działanie, które nie informują w jasny sposób, jak je zamknąć.

① Ta reklama nie zawiera przycisku zamykania.

- Reklamy, które wymuszają na użytkowniku kliknięcie, wyświetlając fałszywy przycisk zamykania lub pojawiając się nagle w obszarach aplikacji, które użytkownik zwykle klika, by użyć innej funkcji.



- Reklama korzystająca z fałszywego przycisku zamknięcia.



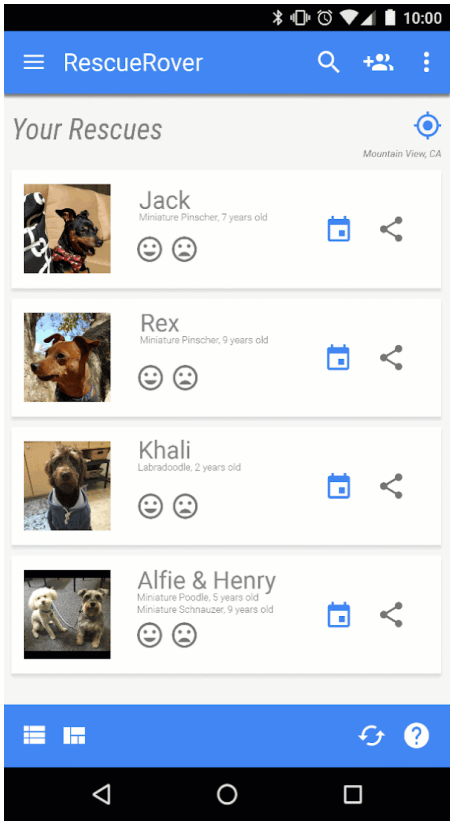
Reklama pojawiająca się nagle w miejscu, które użytkownik z przyzwyczajenia klika, by skorzystać z funkcji aplikacji.

Zakłócanie działania aplikacji, reklam innych firm lub funkcji urządzenia

Reklamy powiązane z aplikacją nie mogą zakłócać działania innych aplikacji, reklam ani pracy urządzenia, w tym jego systemu, przycisków i portów. Dotyczy to też nakładek, funkcji towarzyszących i reklam w formie widżetów. Reklamy mogą wyświetlać się tylko w aplikacji, która je zawiera.

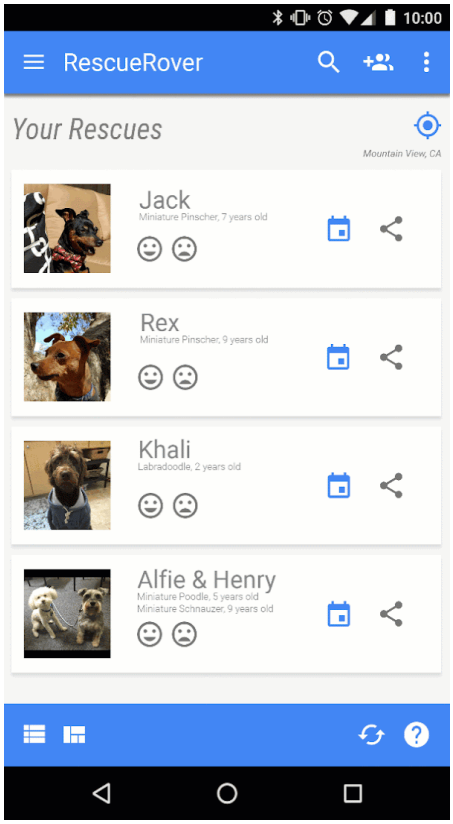
Aby zagwarantować, że platforma Google Play jest bezpiecznym i tolerancyjnym miejscem, stworzyliśmy standardy, które definiują i blokują materiały szkodliwe lub nieodpowiednie dla naszych użytkowników.

- Reklamy wyświetlane poza aplikacją, która je zawiera.



Opis: gdy przechodzi się z aplikacji do ekranu głównego, nagle pojawia się na nim reklama.

- Reklamy wyświetlane po naciśnięciu przycisku ekranu głównego lub użyciu innych funkcji wyraźnie zaprojektowanych do zamykania aplikacji.

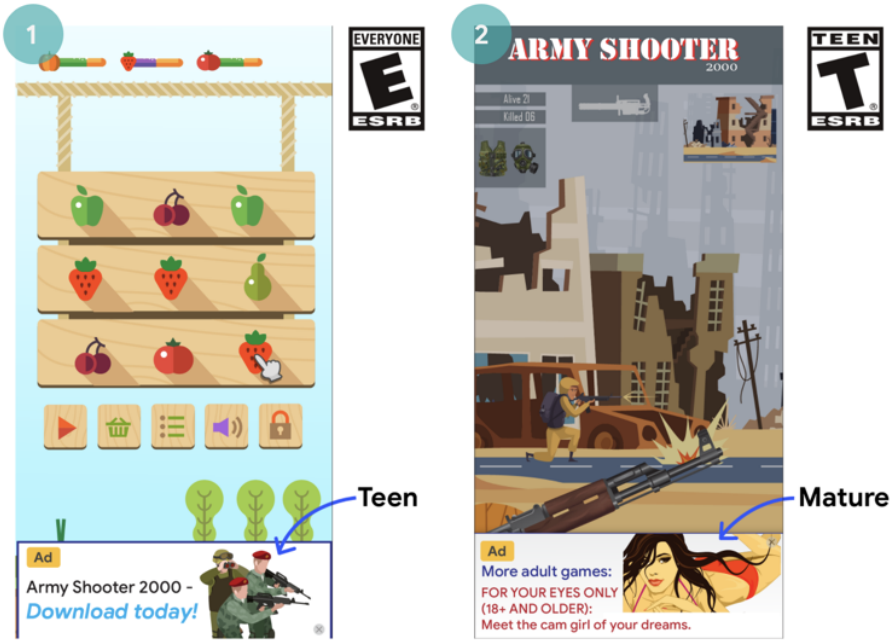


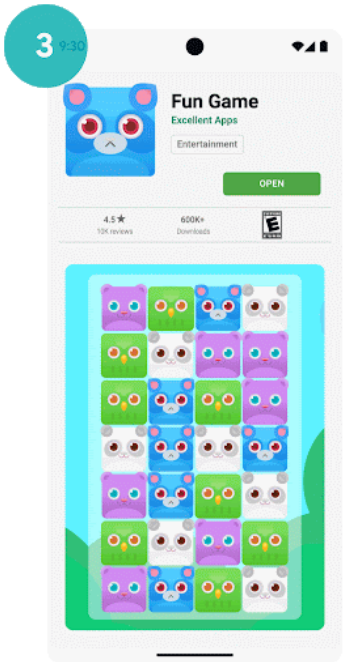
Opis: użytkownik chce wyjść z aplikacji i przejść do ekranu głównego, ale czynność ta jest niespodziewanie przerywana przez wyświetlanie się reklamy.

Nieodpowiednie reklamy

Reklamy i powiązane z nimi oferty (na przykład reklama promująca pobranie innej aplikacji) wyświetlane w Twojej aplikacji muszą być odpowiednie do jej oceny treści , nawet jeśli sama treść jest gólnie zgodna z naszymi zasadami.

Aby zagwarantować, że platforma Google Play jest bezpiecznym i tolerancyjnym miejscem, stworzyliśmy standardy, które definiują i blokują materiały szkodliwe lub nieodpowiednie dla naszych użytkowników.





① Ta reklama (zawierająca treści dla nastolatków) jest nieodpowiednia ze względu na ocenę treści aplikacji (Dla wszystkich).
② Ta reklama (zawierająca treści dla dorosłych) jest nieodpowiednia ze względu na ocenę treści aplikacji (Dla nastolatków).

③ Oferta przedstawiona w reklamie (promującej pobranie aplikacji dla dorosłych) jest nieodpowiednia ze względu na ocenę treści gry mobilnej, w której została wyświetlona (Dla wszystkich).

Używanie identyfikatora wyświetlania reklam na urządzeniach z Androidem

W Usługach Google Play w wersji 4.0 wprowadziliśmy nowe interfejsy API i nowy identyfikator na użytek dostawców usług reklamowych i analitycznych. Warunki korzystania z tego identyfikatora znajdziesz poniżej.

- **Użycie**. Identyfikator wyświetlania reklam na urządzeniach z Androidem (AAID) może być używany jedynie do celów reklamowych i do analizowania informacji o użytkownikach. Stan ustawienia rezygnacji z reklam opartych na zainteresowaniach lub reklam spersonalizowanych musi być weryfikowany przy każdym dostępie do identyfikatora.
- **Powiązanie z informacjami umożliwiającymi identyfikację osoby lub z innymi identyfikatorami.**
  - Wykorzystanie na potrzeby reklam: identyfikatora wyświetlania reklam nie wolno łączyć z trwałymi identyfikatorami urządzeń (takimi jak SSAID, adres MAC, IMEI itp.) na potrzeby jakiejkolwiek formy reklamy. Identyfikator wyświetlania reklam może być połączony z informacjami umożliwiającymi identyfikację tylko za wyraźną zgodą użytkownika.
  - Wykorzystanie na potrzeby analiz: identyfikatora wyświetlania reklam nie wolno łączyć z informacjami umożliwiającymi identyfikację ani wiązać z żadnym stałym identyfikatorem urządzenia (np. identyfikatorem SSAID, adresem MAC, numerem IMEI itp.) na potrzeby jakichkolwiek analiz. Dodatkowe wytyczne na temat trwałych identyfikatorów urządzeń zawierają zasady dotyczące danych użytkownika .
- **Szanowanie decyzji użytkownika.**
  - Po zresetowaniu nowy identyfikator wyświetlania reklam nie może zostać połączony z poprzednim ani z danymi uzyskanymi na podstawie poprzedniego identyfikatora bez wyraźnej zgody użytkownika.
  - Należy stosować się do wybranego przez użytkowników ustawienia rezygnacji z reklam opartych na zainteresowaniach lub reklam spersonalizowanych. Jeśli użytkownik włączył to ustawienie, nie wolno używać identyfikatora wyświetlania reklam do tworzenia profili użytkowników do celów reklamowych ani do kierowania na użytkowników reklam spersonalizowanych. Dozwolone zastosowania obejmują reklamę kontekstową, ograniczanie liczby wyświetleń, śledzenie konwersji, raportowanie, wykrywanie oszustw oraz bezpieczeństwo.
  - Na nowszych urządzeniach identyfikator wyświetlania reklam na Androidzie zostanie usunięty, kiedy użytkownik go usunie. Każda próba odczytania identyfikatora będzie wtedy zwracać ciąg zer. Urządzenia bez identyfikatora wyświetlania reklam nie wolno łączyć z danymi powiązanymi z poprzednim identyfikatorem ani uzyskanymi na jego podstawie.
- **Przejrzystość dla użytkowników.** Informacje o zbieraniu danych i wykorzystaniu identyfikatora wyświetlania reklam oraz zobowiązanie do przestrzegania tych warunków należy przedstawić użytkownikom w powiadomieniu o ochronie prywatności zgodnym z przepisami prawa. Więcej informacji o naszych standardach w zakresie prywatności znajdziesz w zasadach dotyczących danych użytkownika .
- **Przestrzeganie warunków korzystania z identyfikatora.** Identyfikatora wyświetlania reklam można używać tylko zgodnie z Zasadami programu dla deweloperów w Google Play. Obowiązują one też wszystkie firmy, którym udostępniasz identyfikator w ramach prowadzenia działalności. Wszystkie aplikacje przesłane do Google Play lub opublikowane w tej usłudze muszą do celów reklamowych używać identyfikatora wyświetlania reklam (jeśli jest dostępny na urządzeniu) zamiast innych identyfikatorów.

Lepsza jakość reklam

Wymagamy, aby deweloperzy przestrzegali poniższych wytycznych dotyczących reklam, które zapewniają użytkownikom wysoką jakość aplikacji w Google Play. Twoje reklamy mogą nie wyświetlać się w tych nieoczekiwanych dla użytkowników sytuacjach:

- Reklamy pełnoekranowe wszystkich formatów (wideo, GIF, statyczne itp.), które wyświetlają się nieoczekiwanie, zwykle wtedy, gdy użytkownik postanowił zrobić coś innego, są niedozwolone.
  - Reklamy, które pojawiają się w trakcie rozgrywki na początku poziomu lub segmentu treści, są niedozwolone.
  - Pełnoekranowe reklamy wideo, które pojawiają się przed ekranem wczytywania aplikacji (ekranem powitalnym), są niedozwolone.
- Reklamy pełnoekranowe wszystkich formatów (wideo, GIF, statyczne itp.), których nie można zamknąć po 15 sekundach, są niedozwolone. Opcjonalne reklamy pełnoekranowe i reklamy pełnoekranowe, które nie przeszkadzają użytkownikom w działaniach (na przykład wyświetlane w grze po ekranie z wynikiem), mogą być widoczne przez ponad 15 sekund.

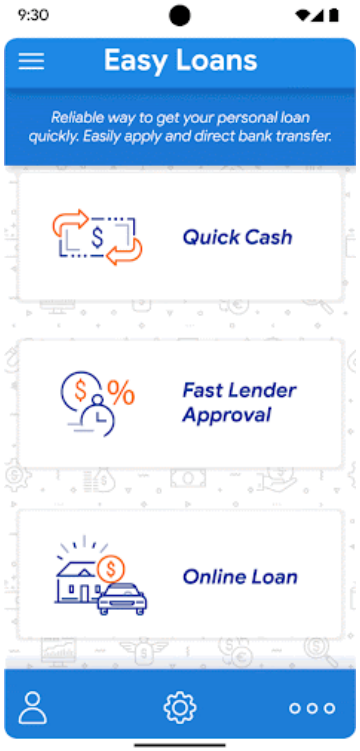
Te zasady nie dotyczą reklam z nagrodą, na których wyświetlenie użytkownik jednoznacznie się zgadza (na przykład reklam, za których obejrzenie deweloperzy wyraźnie oferują użytkownikom odblokowanie funkcji lub treści w grze). Nie dotyczą one także monetyzacji ani reklam, które nie kolidują z normalnym użytkowaniem aplikacji czy przebiegiem rozgrywki w grze (na przykład treści wideo ze zintegrowanymi reklamami czy niepełnoekranowych banerów reklamowych).

Te zasady powstały na podstawie wytycznych Better Ads Standards – Mobile Apps Experiences . Więcej informacji o wytycznych Better Ads Standards znajdziesz w artykule Coalition of Better Ads .

Aby zagwarantować, że platforma Google Play jest bezpiecznym i tolerancyjnym miejscem, stworzyliśmy standardy, które definiują i blokują materiały szkodliwe lub nieodpowiednie dla naszych użytkowników.

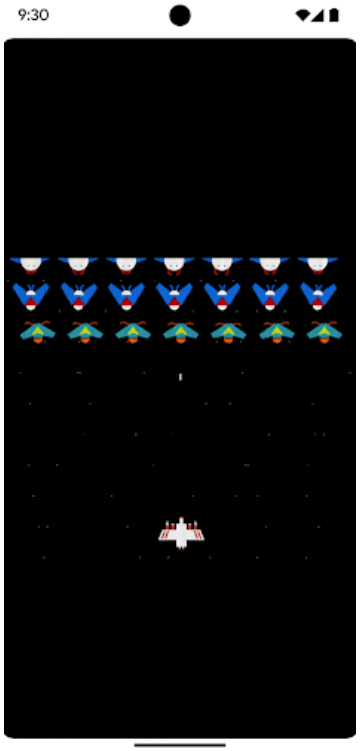
- Nieoczekiwane reklamy, które pojawiają się podczas rozgrywki lub na początku segmentu treści (na przykład po tym, jak użytkownik kliknie przycisk, ale przed wykonaniem akcji, którą to kliknięcie powinno wywołać). Te reklamy są dla użytkowników nieoczekiwane – użytkownik oczekuje, że rozpocznie się gra lub interakcja z treścią, a nie że pojawi się reklama.

① Nieoczekiwana reklama statyczna pojawia się w trakcje rozgrywki, na początku poziomu.



② Nieoczekiwana reklama wideo pojawia się na początku segmentu treści.

- Reklama pełnoekranowa, która pojawia się w trakcie rozgrywki i nie daje się zamknąć po 15 sekundach.



① Reklama pełnoekranowa pojawiają się w trakcie rozgrywki bez opcji pominięcia po 15 sekundach.

Subskrypcje

Deweloper nie może wprowadzać użytkowników w błąd, jeśli chodzi o usługi subskrypcji lub treści oferowane w aplikacji. Informacje o promocjach w aplikacji i na ekranach powitalnych należy przekazywać w sposób przejrzysty. Zabronione jest publikowanie aplikacji, które wprowadzają

użytkowników w błąd lub manipulują nimi w celu zakupu produktów (obejmuje to zakupy w aplikacji i subskrypcje).

Informacje o ofercie muszą być przejrzyste. Dotyczy to wyraźnego przedstawienia warunków oferty, w tym kosztu subskrypcji, cyklu rozliczeniowego i tego, czy subskrypcja jest wymagana do używania aplikacji. Użytkownicy nie powinni być zmuszeni do wykonania dodatkowych czynności w celu sprawdzenia tych informacji.

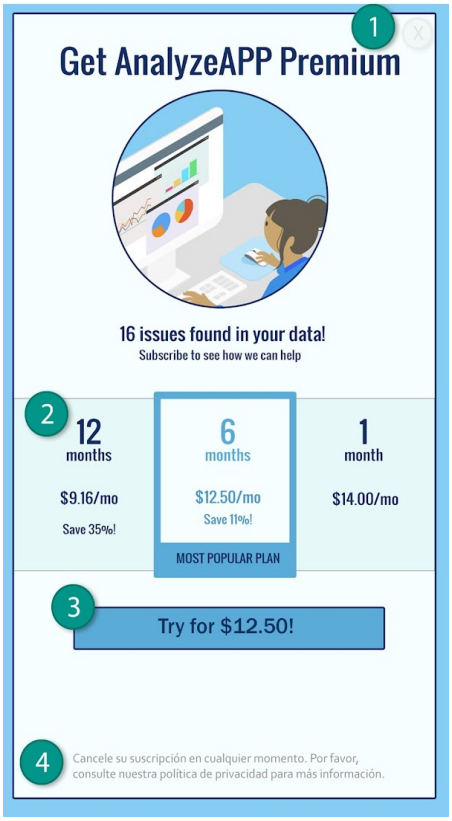
Subskrypcje muszą zapewniać użytkownikom trwałe lub cykliczne korzyści przez cały okres ich obowiązywania. Nie mogą służyć do oferowania użytkownikom korzyści, które w rzeczywistości są jednorazowe (np. kodów SKU umożliwiających jednorazową wypłatę w przypadku waluty lub środków w aplikacji albo jednorazowych bonusów w grze). W ramach subskrypcji mogą być dostępne bonusy motywacyjne lub promocyjne, ale oprócz nich subskrypcja musi przez cały okres obowiązywania zapewniać trwałe lub cykliczne korzyści. W przypadku produktów, które nie wiążą się z trwałymi ani cyklicznymi korzyściami, zamiast subskrypcji należy stosować produkty w aplikacji.

Nie można przedstawiać jednorazowych korzyści jako subskrypcji i w ten sposób wprowadzać użytkowników w błąd. Dotyczy to przekształcania zakupionej subskrypcji w jednorazową ofertę (np. przez anulowanie, wycofywanie lub minimalizowanie korzyści cyklicznej).

Aby zagwarantować, że platforma Google Play jest bezpiecznym i tolerancyjnym miejscem, stworzyliśmy standardy, które definiują i blokują materiały szkodliwe lub nieodpowiednie dla naszych użytkowników.

- Subskrypcje miesięczne, w przypadku których użytkownicy nie są informowani o automatycznym, comiesięcznym obciążeniu płatnością.
- Subskrypcje roczne, w przypadku których najlepiej widoczna jest informacja o ich miesięcznym koszcie.
- Ceny i warunki subskrypcji, które nie są w pełni przetłumaczone.
- Promocje w aplikacji, które nie informują w jasny sposób, że użytkownik może korzystać z treści dostępnych w aplikacji bez kupowania subskrypcji (jeśli jest to możliwe).
- Nazwy SKU nieprawidłowo informujące o rodzaju subskrypcji, np. automatyczna subskrypcja cykliczna o nazwie „Bezpłatna wersja próbna” lub „Wypróbuj członkostwo premium – 3 dni bezpłatnie”.
- Wiele ekranów wyświetlanych w procesie zakupu, które prowadzą do przypadkowego kliknięcia przycisku subskrypcji.
- Subskrypcje, które nie zapewniają trwałych ani cyklicznych korzyści – np. w ramach subskrypcji przez pierwszy miesiąc dostępnych jest 1000 klejnotów, ale w kolejnych miesiącach liczba ta spada do 1 klejnotu.
- Wymaganie od użytkownika wykupienia automatycznie odnawianej subskrypcji w celu zapewnienia jednorazowej korzyści oraz anulowanie subskrypcji użytkownika bez jego prośby po zakupie.

Przykład 1:



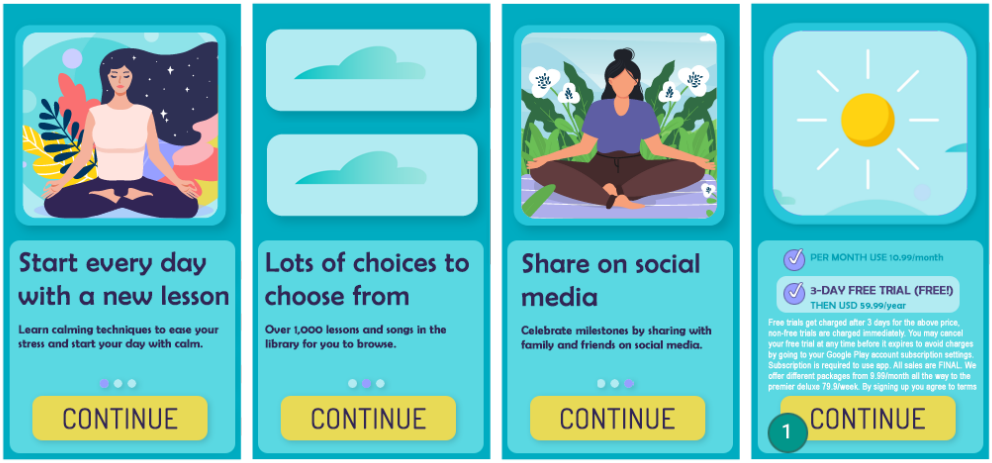
① Przycisk zamykania nie jest wyraźnie widoczny, a użytkownicy mogą nie zrozumieć, że dostęp do funkcji nie wymaga akceptacji oferty subskrypcji.

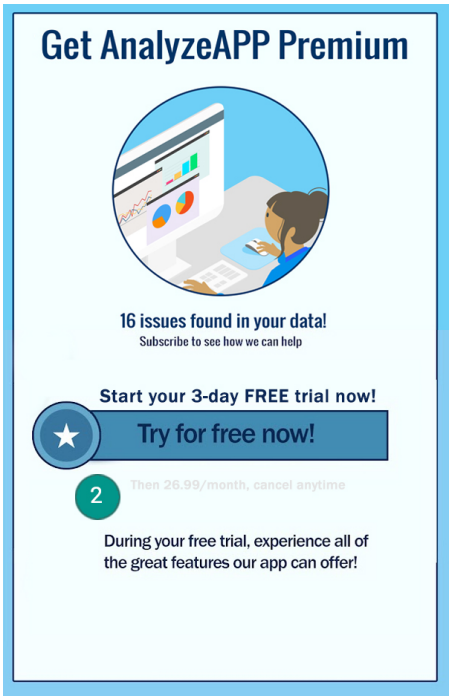
② Oferta zawiera tylko informacje o koszcie miesięcznym, a użytkownicy mogą nie zrozumieć, że w momencie wykupienia subskrypcji zostaną obciążeni opłatą za 6 miesięcy.

③ Oferta zawiera tylko informacje o cenie początkowej, a użytkownicy mogą nie zrozumieć, jakie opłaty będą automatycznie naliczane po okresie początkowym.

④ Oferta powinna być przetłumaczona na ten sam język co warunki usługi, aby użytkownicy mogli wszystko zrozumieć.

Przykład 2:





① Powtarzające się klikanie tego samego obszaru przycisku powoduje niezamierzone kliknięcie ostatniego przycisku „Dalej”, który aktywuje subskrypcję.

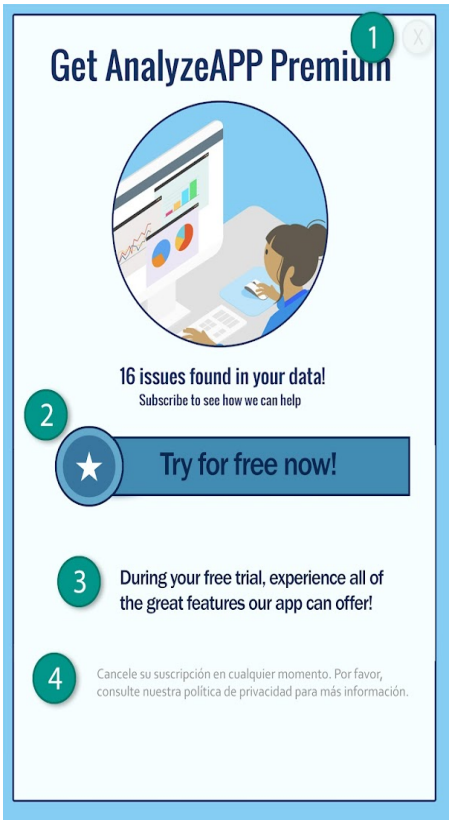
② Trudno odczytać kwotę, którą użytkownik zostanie obciążony po zakończeniu okresu próbnego, przez co użytkownik może mieć wrażenie, że subskrypcja jest bezpłatna.

Bezpłatne wersje próbne i oferty dla nowych subskrybentów

Zanim użytkownik dokona subskrypcji: musisz w jasny i dokładny sposób przedstawić warunki oferty, w tym czas jej trwania i ceny, a także opisać, jakie treści lub usługi są udostępniane. Pamiętaj, by powiadomić użytkowników o sposobie i momencie przejścia z bezpłatnej wersji próbnej na płatną subskrypcję – dodaj też informacje o koszcie oraz możliwości anulowania subskrypcji (jeśli użytkownik nie chce przejść na jej płatną wersję).

Aby zagwarantować, że platforma Google Play jest bezpiecznym i tolerancyjnym miejscem, stworzyliśmy standardy, które definiują i blokują materiały szkodliwe lub nieodpowiednie dla naszych użytkowników.

- Oferty, które nie informują w jasny sposób o tym, jak długo obowiązuje bezpłatny okres próbny lub cena początkowa.
- Oferty, które nie informują w jasny sposób o tym, że użytkownik zostanie automatycznie przeniesiony na płatną subskrypcję po zakończeniu oferty.
- Oferty, które nie informują w jasny sposób, że użytkownik może korzystać z treści dostępnych w aplikacji bez korzystania z wersji próbnej (jeśli jest to możliwe).
- Ceny i warunki oferty nie są w pełni przetłumaczone.



① Przycisk zamykania nie jest wyraźnie widoczny, a użytkownicy mogą nie zrozumieć, że dostęp do funkcji nie wymaga rejestracji i skorzystania z bezpłatnego okresu próbnego.

② Oferta ma wyróżnioną informację o bezpłatnym okresie próbnym, a użytkownicy mogą nie zrozumieć, że po zakończeniu tego okresu będą automatycznie naliczane opłaty.

③ Oferta nie informuje o okresie próbnym, a użytkownicy mogą nie zrozumieć, jak długo będą mieć bezpłatny dostęp do subskrybowanych treści.

④ Oferta powinna być przetłumaczona na ten sam język co warunki usługi, by użytkownicy mogli wszystko zrozumieć.

Zarządzanie subskrypcją i jej anulowanie oraz zwroty środków

Jeśli sprzedajesz w swojej aplikacji subskrypcje, musisz dopilnować, żeby wyraźnie informowała ona, jak użytkownik może tą subskrypcją zarządzać i jak ją anulować. Musisz też zapewnić w aplikacji dostęp do łatwej w użyciu metody anulowania subskrypcji online. Możesz spełnić to wymaganie, dodając w ustawieniach konta aplikacji (lub na podobnej stronie):

- link do Centrum subskrypcji Google Play (w przypadku aplikacji wykorzystujących system rozliczeniowy Google Play); lub
- bezpośredni dostęp do procesu anulowania.

Jeśli użytkownik anuluje subskrypcję kupioną przez system rozliczeniowy Google Play, zgodnie z naszymi ogólnymi zasadami nie otrzyma zwrotu środków za bieżący okres rozliczeniowy, ale może korzystać z subskrybowanych treści do końca tego okresu (niezależnie od daty anulowania subskrypcji). Subskrypcja jest anulowana po upłynięciu bieżącego okresu rozliczeniowego.

Jako dostawca treści lub usługi dostępu możesz wdrożyć bardziej elastyczne zasady zwrotu środków użytkownikom. Ponosisz odpowiedzialność za powiadomienie użytkowników o wszelkich zmianach dotyczących subskrypcji, anulowania i zasad zwrotów oraz za zgodność zasad z obowiązującym prawem.

Program samodzielnej certyfikacji pakietów SDK do wyświetlania reklam dla rodzin

Jeśli Twoja aplikacja jest przeznaczona tylko dla dzieci (zgodnie z definicją zawartą w zasadach dotyczących aplikacji dla rodzin) i wyświetla reklamy, musisz korzystać z pakietów SDK do wyświetlania reklam, które samodzielnie uzyskały certyfikat zgodności z zasadami Google Play, w tym również z poniższymi wymaganiami dotyczącymi samodzielnej certyfikacji pakietów SDK do wyświetlania reklam.

Jeśli aplikacja jest skierowana do dzieci, ale też starszych użytkowników, dopilnuj, żeby reklamy wyświetlane dzieciom pochodziły wyłącznie z któregoś z tych samodzielnie certyfikowanych pakietów SDK do wyświetlania reklam (na przykład zaimplementuj neutralny ekran wyboru wieku). Aplikacje uczestniczące w programie Dla całej rodziny mogą korzystać wyłącznie z samodzielnie certyfikowanych pakietów SDK do wyświetlania reklam.

Pamiętaj, że Twoim obowiązkiem jest dopilnowanie, aby wszystkie wersje pakietów SDK stosowanych w Twojej aplikacji, łącznie z samodzielnie certyfikowanymi pakietami SDK do wyświetlania reklam, były zgodne ze wszystkimi obowiązującymi zasadami oraz lokalnymi przepisami i regulacjami prawnymi. Nie gwarantujemy poprawności informacji podanych przez pakiet SDK do wyświetlania reklam w procesie samodzielnej certyfikacji.

Korzystanie z samodzielnie certyfikowanych pakietów SDK do wyświetlania reklam odpowiednich dla rodzin jest wymagane tylko wtedy, gdy używasz w swojej aplikacji pakietów SDK, żeby wyświetlać reklamy dzieciom. Wymienione poniżej sposoby promocji są dozwolone bez samodzielnej certyfikacji pakietu SDK do wyświetlania reklam w Google Play. Nadal jednak odpowiadasz za to, aby treści Twoich reklam i metody gromadzenia danych były zgodne z zasadami dotyczącymi danych użytkownika i zasadami dotyczącymi aplikacji dla rodzin w Google Play:

- reklamy wewnętrzne, w przypadku których używasz pakietów SDK do zarządzania wzajemną promocją swoich aplikacji lub innych należących do Ciebie mediów i produktów;
- zawieranie umów bezpośrednich z reklamodawcami, gdy korzystasz z pakietów SDK do zarządzania asortymentem.

Wymagania programu samodzielnej certyfikacji pakietów SDK do wyświetlania reklam odpowiednich dla rodzin

- Określ nieodpowiednie treści i zachowania reklam i zakaż ich wyświetlania w warunkach lub zasadach pakietu SDK do wyświetlania reklam. Definicje powinny być zgodne z zasadami programu dla deweloperów w Google Play.
- Utwórz metodę oceny reklam w zależności od tego, do jakich grup wiekowych są kierowane. Musisz uwzględnić co najmniej grupy Dla wszystkich i Dla dorosłych. Metoda oceniania musi odpowiadać tej, którą Google przekazuje dostawcom pakietów SDK po wypełnieniu przez nich formularza zainteresowania (poniżej).
- Zezwól wydawcom, by mogli prosić o traktowanie reklam jako skierowanych do dzieci (jednorazowo lub w całej aplikacji). Takie traktowanie musi być zgodne z obowiązującymi przepisami i regulacjami, takimi jak amerykańska ustawa o ochronie prywatności dzieci w internecie (Children's Online Privacy and Protection Act, COPPA) i unijne Ogólne rozporządzenie o ochronie danych (RODO) . W przypadku traktowania reklam lub aplikacji jako skierowanych do dzieci Google Play wymaga również wyłączenia reklam spersonalizowanych, reklam opartych na zainteresowaniach i remarketingu.
- Pozwól wydawcom wybrać formaty reklam zgodne z zasadami Google Play dotyczącymi zarabiania i reklam wyświetlanych rodzinom oraz zasadami Programu aplikacji zatwierdzonych przez nauczycieli .
- Jeśli przy wyświetlaniu reklam dzieciom używane jest określanie stawek w czasie rzeczywistym, upewnij się, że kreacje zostały sprawdzone, a wskaźniki prywatności zostały przekazane do systemów licytujących.

- Przekaż Google informacje wystarczające do zweryfikowania zgodności pakietu SDK do wyświetlania reklam ze wszystkimi wymogami samodzielnej certyfikacji, takie jak aplikacja testowa i informacje wskazane w poniższym formularzu zgłoszenia zainteresowania , oraz w wyznaczonym czasie odpowiadaj na wszelkie prośby o dodatkowe informacje, np. o przesłanie nowych wersji w celu zweryfikowania zgodności wersji pakietu SDK do wyświetlania reklam ze wszystkimi wymogami samodzielnej certyfikacji.
- Przeprowadź samodzielną certyfikację , aby potwierdzić, że wszystkie nowe wersje są zgodne z najnowszymi zasadami programu dla deweloperów w Google Play, łącznie z wymaganiami opisanymi w zasadach dotyczących aplikacji dla rodzin.

Uwaga: samodzielnie certyfikowane pakiety SDK do wyświetlania reklam odpowiednich dla rodzin muszą wyświetlać reklamy zgodnie ze wszystkimi odpowiednimi przepisami i regulacjami dotyczącymi dzieci (które mogą obowiązywać wydawców reklam).

Oto wymagania dotyczące zapośredniczenia w przypadku platform wyświetlających reklamy dzieciom:

- Używaj wyłącznie samodzielnie certyfikowanych pakietów SDK do wyświetlania reklam odpowiednich dla rodzin lub zaimplementuj środki ochrony, które zagwarantują spełnianie wszystkich tych wymagań przez reklamy pochodzące z zapośredniczenia.
- Przekaż informacje potrzebne platformom zapośredniczenia do wskazania oceny treści reklam i – w razie potrzeby – oznaczenia reklamy jako skierowanej do dzieci.

Lista samodzielnie certyfikowanych pakietów SDK do wyświetlania reklam odpowiednich dla rodzin znajduje się tutaj .

Możesz też udostępnić ten formularz zgłoszenia zainteresowania dostawcom pakietów SDK reklam, którzy chcą przejść samodzielną certyfikację.

Informacje o aplikacji i reklama

Reklama i widoczność aplikacji w znacznym stopniu wpływają na jakość sklepu. Nie publikuj spamu w informacjach o aplikacji, nie wyświetlaj reklam niskiej jakości i nie próbuj sztucznie zwiększyć widoczności aplikacji w Google Play.

Reklama aplikacji

Zabronione jest publikowanie aplikacji biorących w sposób bezpośredni lub pośredni udział w praktykach promocyjnych lub czerpiących z nich korzyści (np. reklam), które wprowadzają w błąd użytkownika albo dewelopera bądź są dla nich szkodliwe. Praktyki promocyjne są uznawane za wprowadzające w błąd lub szkodliwe, jeśli naruszają nasze Zasady programu dla deweloperów.

Przykłady częstych naruszeń:

- wyświetlanie w witrynach, aplikacjach i usługach reklam wprowadzających w błąd , w tym powiadomień, które symulują powiadomienia lub alerty systemu;
- wykorzystywanie reklam o charakterze seksualnym w celu skierowania użytkowników do informacji o aplikacji w Google Play i nakłonienia ich do pobrania aplikacji;
- stosowanie metod promocji lub instalacji przekierowujących użytkowników do Google Play lub powodujących pobieranie aplikacji bez świadomego udziału użytkownika;
- rozsyłanie niechcianych SMS-ów promocyjnych.

Obowiązkiem dewelopera jest dopilnowanie, aby wszelkie sieci reklamowe, podmioty stowarzyszone lub reklamy powiązane z jego aplikacją przestrzegały tych zasad.

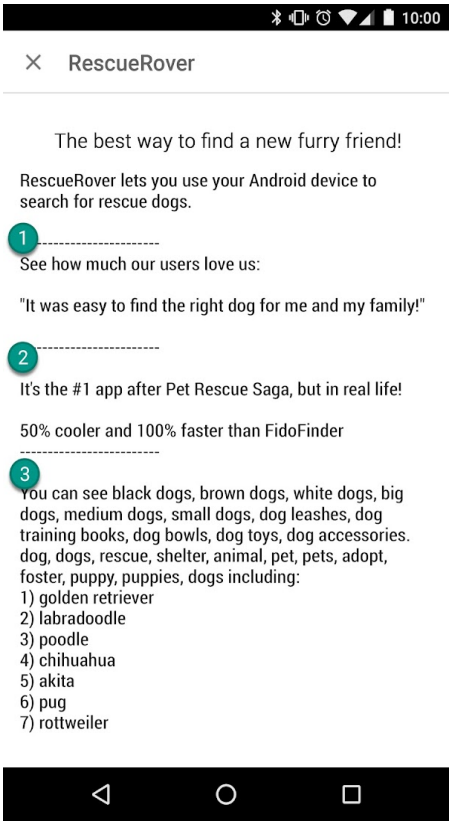
Metadane

Zabraniamy publikowania aplikacji z wprowadzającymi w błąd, nieprawidłowo sformatowanymi, nieopisowymi, nieistotnymi, nadmiernymi lub nieodpowiednimi metadanymi, zawierającymi m.in. opis aplikacji, nazwę dewelopera, tytuł, ikonę, zrzut ekranu i obrazy promocyjne. Deweloperzy muszą przekazać zrozumiały i poprawnie sformułowany opis. Niedozwolone są również niepodpisane lub anonimowe opinie użytkowników w opisie aplikacji.

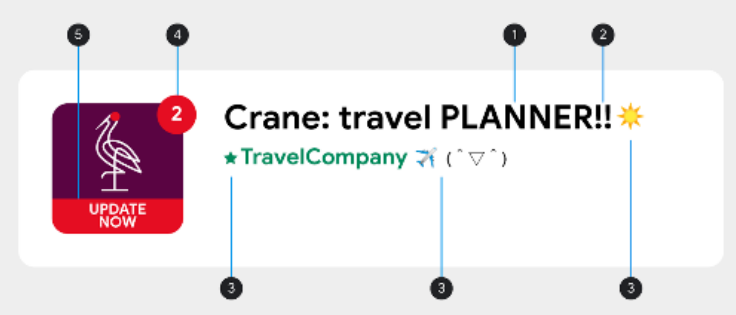
To głównie po tytule i ikonie aplikacji oraz nazwie dewelopera użytkownicy mogą znaleźć Twoją aplikację. W tych elementach metadanych nie używaj emotikonów ani powtarzających się znaków specjalnych. Unikaj WIELKICH LITER, chyba że stanowią część nazwy marki. W ikonach aplikacji niedozwolone są wprowadzające w błąd symbole, np. wskaźnik nowej wiadomości, gdy nie ma nowych wiadomości, czy symbole pobierania/instalowania, gdy aplikacja nie jest związana z pobieraniem treści. Tytuł aplikacji może mieć maksymalnie 30 znaków.

Oprócz wymienionych tutaj wymagań określone Zasady dla deweloperów w Google Play mogą wymagać podania dodatkowych informacji o metadanych.

Aby zagwarantować, że platforma Google Play jest bezpiecznym i tolerancyjnym miejscem, stworzyliśmy standardy, które definiują i blokują materiały szkodliwe lub nieodpowiednie dla naszych użytkowników.



① Niepodpisane lub anonimowe opinie użytkowników
② Porównanie danych o aplikacjach lub markach
③ Bloki słów i pionowe/poziome listy słów



① WIELKIE LITERY, które nie stanowią części nazwy marki
② Sekwencje znaków specjalnych, które są niezwiązane z aplikacją
③ Emotikony (w tym japońskie emotikony) i znaki specjalne
④ Wprowadzające w błąd symbole
⑤ Wprowadzający w błąd tekst

Oto kilka przykładów nieodpowiednich tekstów, obrazów lub filmów w informacjach o aplikacji:

- Obrazy lub filmy o zabarwieniu erotycznym. (unikaj materiałów graficznych – zarówno ilustracji, jak i zdjęć czy filmów – oraz innych treści przedstawiających w dwuznaczny sposób piersi, pośladki, genitalia lub inne części ciała występujące w roli fetysza);
- używanie w informacjach o aplikacji wulgaryzmów, przekleństw lub innych określeń nieodpowiednich dla wszystkich odbiorców;
- drastyczna przemoc wyeksponowana w ikonach aplikacji lub promocyjnych obrazach czy filmach;
- przedstawianie zażywania narkotyków i innych nielegalnych substancji Nawet treści popularnonaukowe, dokumentalne, naukowe i artystyczne zawarte w informacjach o aplikacji muszą być odpowiednie dla wszystkich odbiorców.

Oto kilka sprawdzonych metod:

- Podkreśl zalety aplikacji. Podziel się z użytkownikami ciekawymi, zachęcającymi uwagami o aplikacji, by pokazać im, co ją wyróżnia.
- Dopilnuj, by tytuł i opis aplikacji dokładnie informowały o jej funkcjach.
- Unikaj powtarzających się lub niepowiązanych z aplikacją słów kluczowych i odwołań.
- Opis aplikacji powinien być jasny i zwięzły. Na urządzeniach z mniejszymi ekranami z reguły lepiej sprawdzają się krótsze opisy. Zbyt długi, szczegółowy, nieprawidłowo sformatowany lub pełen powtórzeń opis może naruszać nasze zasady.
- Pamiętaj, że informacje o aplikacji muszą być odpowiednie dla ogółu odbiorców. Nie zamieszczaj w nich nieodpowiednich tekstów, obrazów ani filmów. Pamiętaj też o konieczności przestrzegania wymienionych wyżej wytycznych.

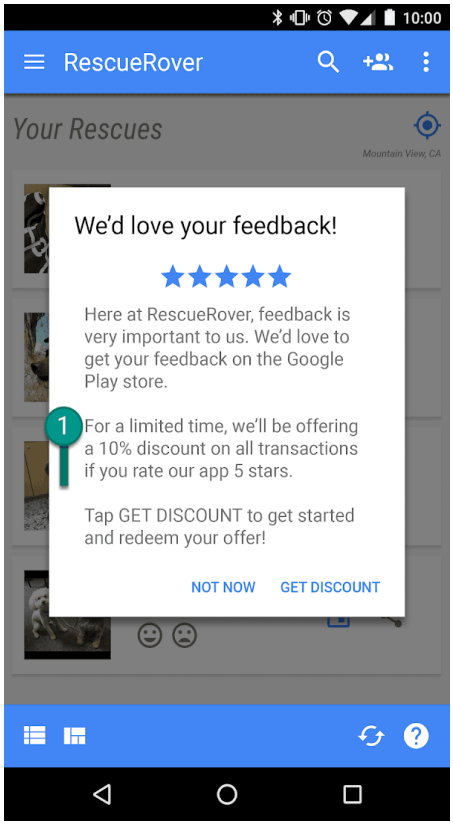
Instalacje, opinie i oceny użytkowników

Deweloperzy nie mogą próbować zmienić pozycji żadnej aplikacji w Google Play. Obejmuje to między innymi podwyższanie ocen produktów i liczby instalacji oraz zamieszczanie opinii przy użyciu nielegalnych praktyk, takich jak fałszywe lub generowane przez zachęty instalacje, opinie czy oceny. Zachęty wpływające na instalacje, opinie lub oceny obejmują teksty i obrazy w tytule czy ikonie aplikacji lub nazwie dewelopera, które zawierają cenę lub inne informacje promocyjne.

Deweloperzy nie mogą dodawać w tytule czy ikonie aplikacji ani nazwie dewelopera tekstów ani grafik, które sugerują wysoką sprzedaż lub pozycję w rankingu albo związek z aktualnymi programami w Google Play.

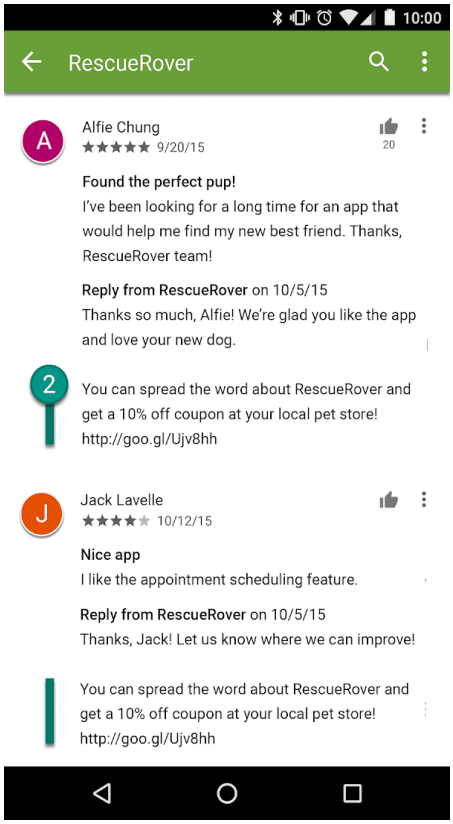
Aby zagwarantować, że platforma Google Play jest bezpiecznym i tolerancyjnym miejscem, stworzyliśmy standardy, które definiują i blokują materiały szkodliwe lub nieodpowiednie dla naszych użytkowników.

- Oferowanie użytkownikom korzyści w zamian za wystawienie oceny:



① To powiadomienie proponuje użytkownikom zniżkę w zamian za wysoką ocenę.

- Wielokrotne przesyłanie ocen, by wpłynąć na pozycję aplikacji w Google Play.
- Zgłaszanie lub zachęcanie użytkowników do zamieszczania opinii z nieodpowiednimi treściami, w tym poprzez informacje o podmiotach stowarzyszonych, kupony, kody do gier, adresy e-mail czy linki do witryn lub innych aplikacji:



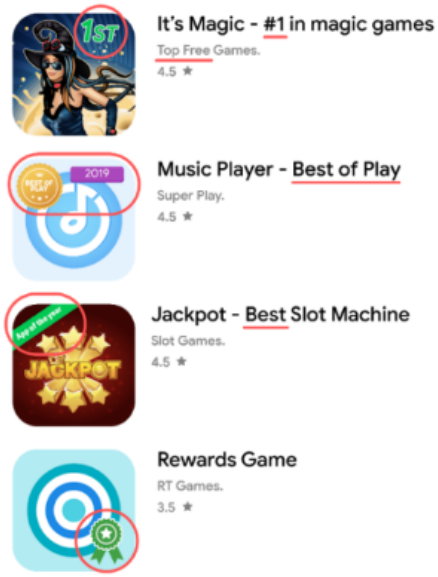
② Ta opinia zachęca użytkowników do promowania aplikacji RescueRover przez oferowanie kuponów.

Oceny i opinie są wskaźnikami jakości aplikacji. Użytkownicy oczekują, że będą one autentyczne i wiarygodne. Oto niektóre ze sprawdzonych metod odpowiadania na opinie użytkowników:

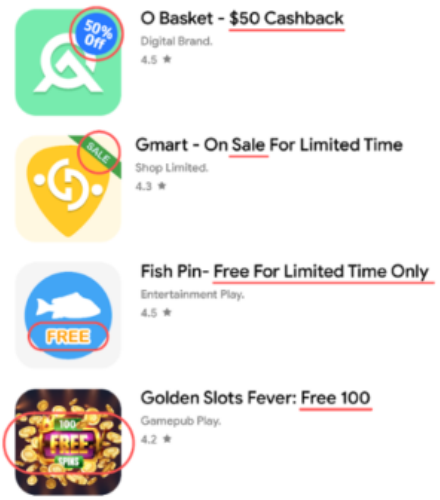
- Skup się na problemach wskazanych w komentarzu użytkownika i nie proś o wyższą ocenę.
- Wskaż materiały, które mogą się przydać – np. e-mail do pomocy technicznej czy adres strony z najczęstszymi pytaniami.

Aby zagwarantować, że platforma Google Play jest bezpiecznym i tolerancyjnym miejscem, stworzyliśmy standardy, które definiują i blokują materiały szkodliwe lub nieodpowiednie dla naszych użytkowników.

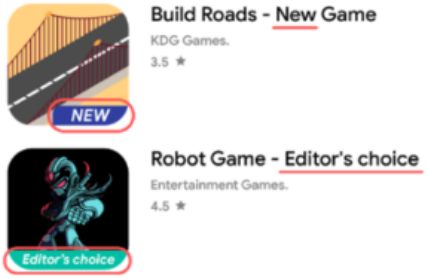
- grafiki i teksty sugerujące wysoką sprzedaż lub pozycję w rankingu (np. „Aplikacja roku”, „Numer 1”, „Najlepsza w Google Play w 20XX”, „Popularna”, ikony nagród itp.);



- grafiki lub teksty zawierające cenę lub informacje promocyjne (np. „10% taniej”, „50 zł zwrotu”, „Bezpłatnie tylko przez ograniczony czas” itp.);



- grafiki lub teksty nawiązujące do programów Google Play (np. „Nasz wybór”, „Nowe” itp).



Oceny treści

System oceny treści w Google Play powstał, by deweloperzy mogli udostępniać użytkownikom na całym świecie wiarygodne oceny uwzględniające uwarunkowania lokalne. Systemem ocen zarządza organizacja International Age Rating Coalition (IARC) . Regionalne oddziały IARC publikują wytyczne, które służą do określania poziomu dojrzałości użytkowników aplikacji. W Google Play nie wolno publikować aplikacji bez oceny treści.

Do czego używane są oceny treści

Oceny treści mają za zadanie informować klientów (zwłaszcza rodziców) o potencjalnie nieodpowiednich treściach w aplikacjach. Pomagają też blokować lub odfiltrowywać treści w niektórych krajach/regionach lub dla określonych użytkowników, gdy wymaga tego prawo, oraz ocenić możliwość włączenia aplikacji do specjalnych programów dla deweloperów.

W jaki sposób nadawane są oceny

Aby otrzymać ocenę treści, musisz wypełnić kwestionariusz oceny w Konsoli Play i opisać treści dostępne w aplikacji. Na podstawie odpowiedzi udzielonych w kwestionariuszu różne organizacje oceniające nadają Twojej aplikacji ocenę treści. Fałszywe przedstawienie zawartości aplikacji może spowodować jej usunięcie lub zawieszenie – odpowiedz jak najdokładniej na pytania w kwestionariuszu oceny treści.

Aby uniknąć wyświetlania aplikacji „Bez oceny”, wypełnij kwestionariusz oceny treści każdej nowej aplikacji przesłanej do Konsoli Play, a także wszystkich istniejących aplikacji, które są aktywne w Google Play. Aplikacje bez oceny treści będą usuwane ze Sklepu Play.

Jeśli wprowadzisz w aplikacji aktualizacje, które zmienią jej zawartość lub funkcje i mogą wpłynąć na odpowiedzi udzielone w kwestionariuszu oceny treści w Konsoli Play, musisz przesłać nowy kwestionariusz.

Informacje o organizacjach oceniających oraz instrukcje wypełniania kwestionariusza oceny treści znajdziesz w Centrum pomocy .

Zgłaszanie odwołań od ocen

Jeśli nie zgadzasz się z oceną nadaną Twojej aplikacji, możesz odwołać się bezpośrednio do organizacji oceniającej IARC, korzystając z linku podanego w e-mailu z certyfikatem.

Wiadomości

Aplikacja prezentująca wiadomości to aplikacja, która:

- jest określona w Konsoli Google Play jako „aplikacja prezentująca wiadomości”;
- należy do kategorii „Wiadomości i czasopisma” w Sklepie Google Play i jest określona jako „wiadomości” w tytule, ikonie, nazwie dewelopera lub opisie.

Przykłady aplikacji z kategorii „Wiadomości i czasopisma”, które kwalifikują się jako aplikacje prezentujące wiadomości:

- aplikacje określone jako „wiadomości” w opisie aplikacji, między innymi:
  - najnowsze wiadomości;
  - gazeta;
  - aktualności;
  - wiadomości lokalne;
  - wiadomości dnia;
- aplikacje mające słowo „wiadomości” w tytule, ikonie lub nazwie dewelopera.

Aplikacje, które zawierają przede wszystkim treści użytkowników (np. aplikacje mediów społecznościowych), nie powinny być określane jako aplikacje prezentujące wiadomości i nie są uznawane za takie aplikacje.

Aplikacje prezentujące wiadomości, które wymagają od użytkownika wykupienia subskrypcji, muszą przed zakupem umożliwiać użytkownikom wyświetlenie podglądu treści w aplikacji.

Aplikacje prezentujące wiadomości muszą:

- Zawierać informacje o wydawcy aplikacji i źródle artykułów z wiadomościami, w tym między innymi o wydawcy lub autorze każdego artykułu. W sytuacji, gdy wskazywanie indywidualnych autorów artykułów nie jest przyjętą normą, aplikacja prezentująca wiadomości musi być wydawcą tych artykułów. Przypominamy, że linki do kont w mediach społecznościowych nie stanowią wystarczających informacji o autorze lub wydawcy.
- Mieć specjalną witrynę lub stronę w aplikacji oznaczoną wyraźnie jako miejsce podania informacji kontaktowych, która jest łatwa do zlokalizowania (np. za pomocą linku na dole strony głównej lub na pasku nawigacyjnym) i zawiera prawidłowe informacje kontaktowe wydawcy wiadomości, w tym adres e-mail lub numer telefonu do kontaktu. Przypominamy, że linki do kont w mediach społecznościowych nie stanowią wystarczających informacji kontaktowych wydawcy.

Aplikacje prezentujące wiadomości nie mogą:

- Zawierać poważnych błędów ortograficznych ani gramatycznych.
- Prezentować wyłącznie treści statycznych (np. sprzed 3 miesięcy).
- Mieć za główny cel marketingu afiliacyjnego ani generowania przychodów z reklam.

Aplikacje prezentujące wiadomości *mogą* używać reklam i innych form promocji, aby osiągać przychody, o ile głównym celem aplikacji nie jest sprzedaż produktów lub usług ani generowanie przychodów z reklam.

Aplikacje prezentujące wiadomości i gromadzące treści z różnych źródeł muszą jasno informować o źródle publikującym poszczególne materiały prezentowane w aplikacji, a każde ze źródeł musi spełniać wymagania określone w zasadach Wiadomości.

Z tego artykułu dowiesz się, jak podać wymagane informacje.

Spam i minimalna funkcjonalność

Aplikacje powinny zapewniać użytkownikom przynajmniej minimalny poziom funkcjonalności i wygody użytkowania. Aplikacje zawierające błędy, odznaczające się niską wygodą obsługi albo służące tylko do rozpowszechniania spamu wśród użytkowników lub w Google Play nie przyczyniają się do znaczącego wzbogacenia katalogu.

Spam

Zabronione jest publikowanie aplikacji rozpowszechniających spam wśród użytkowników lub w Google Play, w tym aplikacji, które wysyłają niechciane wiadomości, oraz takich, które są powieleniem innych i charakteryzują się niską jakością.

Spam w wiadomościach

Zabronione jest publikowanie aplikacji wysyłających SMS-y, e-maile lub inne wiadomości w imieniu użytkownika bez możliwości potwierdzenia przez niego ich treści i adresatów.

Aby zagwarantować, że platforma Google Play jest bezpiecznym i tolerancyjnym miejscem, stworzyliśmy standardy, które definiują i blokują materiały szkodliwe lub nieodpowiednie dla naszych użytkowników.

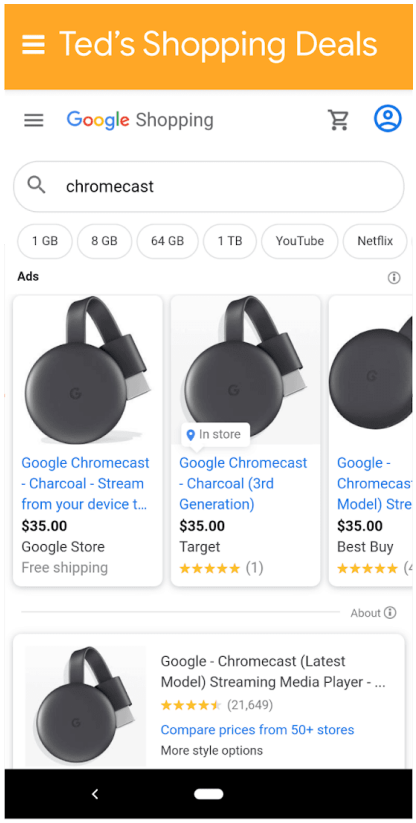
- Gdy użytkownik klika przycisk „Udostępnij”, aplikacja wysyła w jego imieniu wiadomości bez możliwości potwierdzenia przez niego ich treści i adresatów:

Spam związany z wyświetleniami witryn i podmiotami stowarzyszonymi

Zabronione jest publikowanie aplikacji, których głównym przeznaczeniem jest zwiększanie ruchu do powiązanej z nią witryny lub generowanie widoku witryny bez pozwolenia jej właściciela lub administratora.

Aby zagwarantować, że platforma Google Play jest bezpiecznym i tolerancyjnym miejscem, stworzyliśmy standardy, które definiują i blokują materiały szkodliwe lub nieodpowiednie dla naszych użytkowników.

- Aplikacja, której głównym celem jest zwiększanie ruchu do witryny w celu otrzymywania środków za rejestracje użytkowników lub zakupy w tej witrynie.
- Aplikacje, których głównym przeznaczeniem jest generowanie widoku witryny bez pozwolenia:



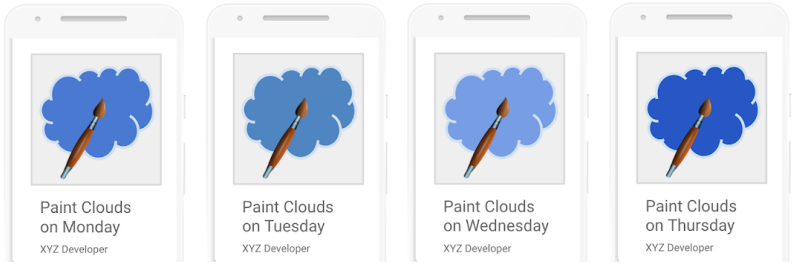
① Aplikacja o nazwie „Ted's Shopping Deals" generuje jedynie widok strony z Zakupów Google.

Powielanie treści

Zabronione jest publikowanie aplikacji, które jedynie powielają treści i funkcje innych aplikacji dostępnych już w Google Play. Aplikacje muszą oferować użytkownikom unikalne treści, funkcje lub usługi.

Aby zagwarantować, że platforma Google Play jest bezpiecznym i tolerancyjnym miejscem, stworzyliśmy standardy, które definiują i blokują materiały szkodliwe lub nieodpowiednie dla naszych użytkowników.

- Kopiowanie treści z innych aplikacji bez dodania czegoś oryginalnego.
- tworzenie wielu aplikacji o bardzo podobnej zawartości i sposobie działania czy funkcjach Jeśli każda z aplikacji zawiera mało treści, deweloperzy powinni raczej udostępnić wszystkie treści w jednej aplikacji.

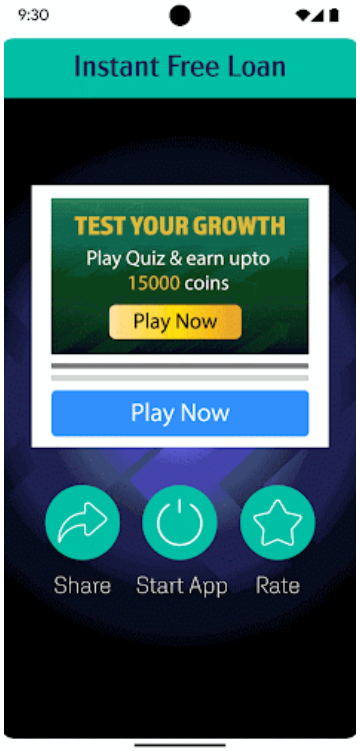


Aplikacje, które mają przede wszystkim wyświetlać reklamy

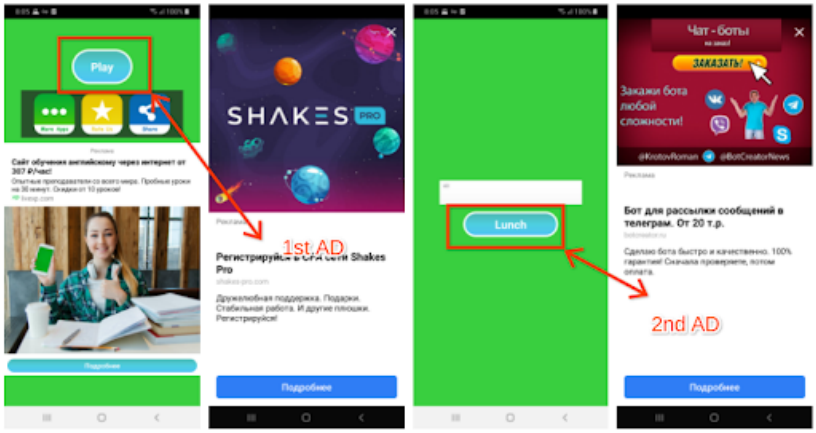
Zabraniamy publikowania aplikacji, które wielokrotnie wyświetlają reklamy pełnoekranowe rozpraszające użytkownika i utrudniające mu interakcję z aplikacją lub wykonywanie w niej zadań.

Aby zagwarantować, że platforma Google Play jest bezpiecznym i tolerancyjnym miejscem, stworzyliśmy standardy, które definiują i blokują materiały szkodliwe lub nieodpowiednie dla naszych użytkowników.

- Aplikacje, w których reklama pełnoekranowa jest wielokrotnie wyświetlana po wykonaniu przez użytkownika jakiejś czynności (w tym także po kliknięciu lub przesunięciu palcem).



Pierwsza strona w aplikacji ma wiele przycisków, z którymi można wejść w interakcję. Gdy użytkownik klika **Uruchom aplikację** (Start app), aby zacząć korzystać z aplikacji, pojawia się reklama pełnoekranowa. Po zamknięciu reklamy użytkownik wraca do aplikacji i klika **Usługa**(Service), aby zacząć korzystać z usługi, ale pojawia się kolejna reklama pełnoekranowa.



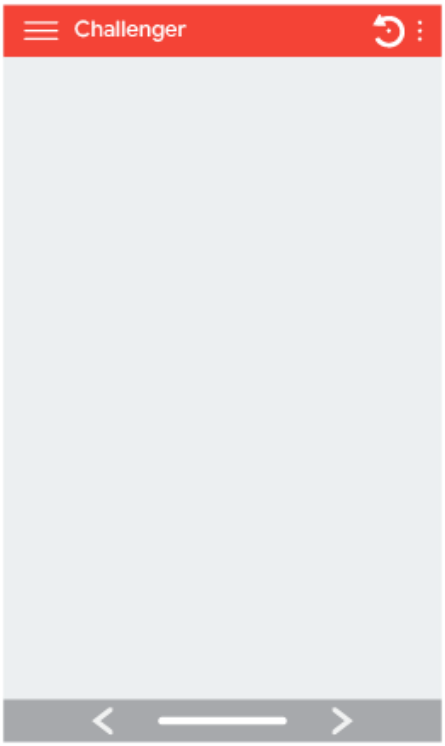
Na pierwszej stronie użytkownik musi kliknąć **Zagraj** (Play), ponieważ jest to jedyny dostępny przycisk umożliwiający użycie aplikacji. Gdy użytkownik go klika, pojawia się reklama pełnoekranowa. Po zamknięciu reklamy użytkownik klika **Uruchom** (Launch), ponieważ jest to jedyny przycisk, z którym może wejść w interakcję, po czym pojawia się kolejna reklama pełnoekranowa.

Minimalna funkcjonalność

Zadbaj o to, by aplikacja działała stabilnie i dostatecznie szybko, a sposób prezentowania treści był atrakcyjny i angażujący.

Aby zagwarantować, że platforma Google Play jest bezpiecznym i tolerancyjnym miejscem, stworzyliśmy standardy, które definiują i blokują materiały szkodliwe lub nieodpowiednie dla naszych użytkowników.

- Aplikacje, które zostały tak opracowane, by nie wykonywać żadnych działań, lub nie mają żadnych funkcji



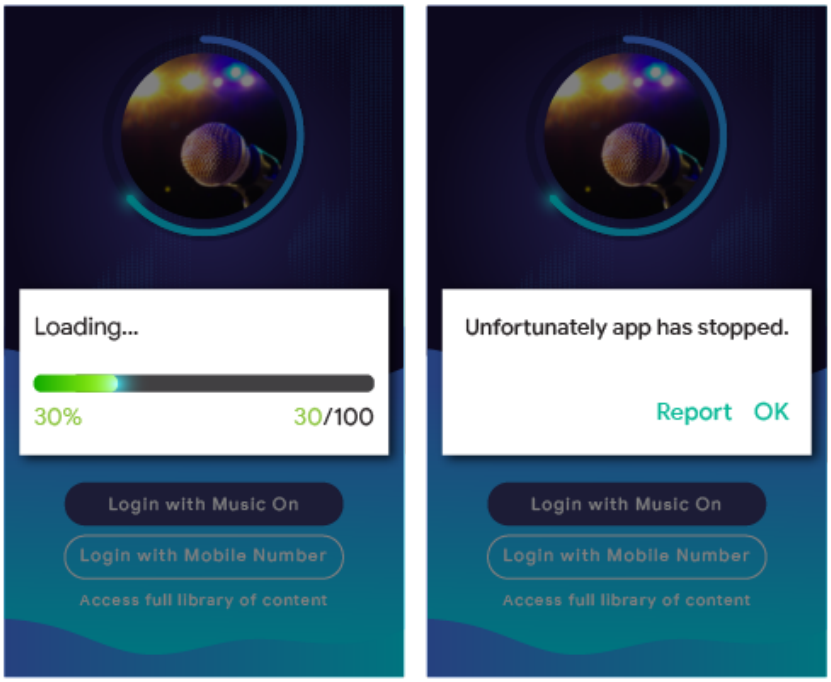
Nieprawidłowe działanie

Zabronione jest publikowanie aplikacji z błędami, wymuszających zamknięcia, blokujących się lub działających nieprawidłowo.

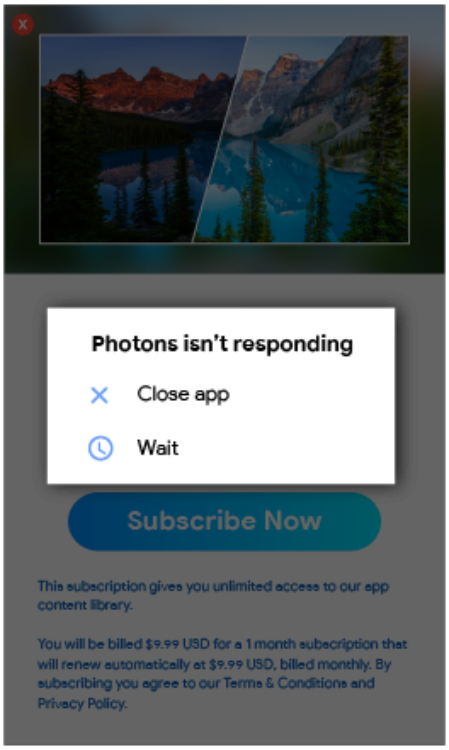
Aby zagwarantować, że platforma Google Play jest bezpiecznym i tolerancyjnym miejscem, stworzyliśmy standardy, które definiują i blokują materiały szkodliwe lub nieodpowiednie dla naszych użytkowników.

- Aplikacje, których **nie można zainstalować**.

- Aplikacje, które można zainstalować, ale które **się nie ładują**



- Aplikacje, które się ładują, ale **nie odpowiadają**



Inne programy

Poza zgodnością z polityką treści, określoną w innym miejscu w tym Centrum zasad, aplikacje stworzone z myślą o innych sposobach korzystania z Androida i udostępniane w Google Play mogą

również podlegać wymogom dotyczącym konkretnego programu. Zapoznaj się z poniższą listą, by sprawdzić, czy któreś z tych zasad dotyczą Twojej aplikacji.

Aplikacje błyskawiczne na Androida

Chcemy, by aplikacje błyskawiczne na Androida były wygodne i bezproblemowe w obsłudze, a jednocześnie zgodne z najwyższymi standardami prywatności i bezpieczeństwa. Właśnie w tym celu opracowaliśmy nasze zasady.

Deweloperzy, którzy decydują się udostępniać aplikacje błyskawiczne na Androida w Google Play, oprócz pozostałych Zasad programu dla deweloperów w Google Play muszą przestrzegać tych zasad.

Tożsamość

W aplikacjach, które zawierają funkcję logowania, deweloperzy muszą zastosować Smart Lock na hasła .

Obsługa linków

Deweloperzy aplikacji błyskawicznych na Androida muszą zapewnić prawidłową obsługę linków do innych aplikacji. Jeśli aplikacje błyskawiczne lub instalowane zawierają linki, które mogą prowadzić do aplikacji błyskawicznej, deweloper musi kierować użytkowników do tej aplikacji błyskawicznej, a nie np. rejestrować linki w WebView .

Specyfikacje techniczne

Deweloperzy muszą przestrzegać specyfikacji technicznych aplikacji błyskawicznych na Androida i określonych przez Google wymagań (również tych wymienionych w naszej dokumentacji publicznej), które co jakiś czas mogą się zmieniać.

Opcja zainstalowania aplikacji

Aplikacja błyskawiczna może oferować użytkownikowi wersję do zainstalowania, ale nie może to być jej głównym przeznaczeniem. Oferując wersję instalowaną, deweloperzy:

- muszą użyć ikony „Pobierz aplikację” w stylu Material Design i etykiety „Zainstaluj” na przycisku instalacji;
- nie mogą zamieszczać w aplikacji błyskawicznej więcej niż 2–3 wiadomości nakłaniających do instalacji;
- nie mogą używać banerów ani innych technik reklamowych do przedstawiania użytkownikom wiadomości zachęcających do instalacji.

Dodatkowe informacje o aplikacjach błyskawicznych i wskazówki dotyczące UX znajdziesz w artykule o sprawdzonych metodach zwiększania wygody użytkowników .

Zmiana stanu urządzenia

Aplikacje błyskawiczne nie mogą wprowadzać na urządzeniu zmian, które utrzymują się dłużej niż sesja takiej aplikacji. Na przykład aplikacje nie mogą zmieniać tapety użytkownika ani tworzyć widżetów na ekranie głównym.

Widoczność aplikacji

Deweloperzy muszą zapewnić użytkownikom widoczność aplikacji błyskawicznych, tak by użytkownik przez cały czas wiedział, że na urządzeniu działa taka aplikacja.

Identyfikatory urządzeń

Aplikacje błyskawiczne nie mogą uzyskiwać dostępu do identyfikatorów urządzeń, które: (1) utrzymują się po zakończeniu działania aplikacji błyskawicznej; (2) nie mogą być resetowane przez użytkownika. Wybrane przykłady:

- numery seryjne kompilacji,
- adresy MAC jakichkolwiek układów sieciowych,
- numery IMEI lub IMSI.

Aplikacje błyskawiczne mogą uzyskiwać dostęp do numeru telefonu, który został uzyskany na podstawie uprawnień podczas działania. Deweloper nie może próbować identyfikować użytkownika za pomocą takich identyfikatorów lub innych metod.

Ruch w sieci

Ruch sieciowy wychodzący z aplikacji błyskawicznej musi być szyfrowany przy użyciu protokołu TLS, takiego jak HTTPS.

Zasady dotyczące emotikonów systemu Android

Nasze zasady dotyczące emotikonów zostały opracowane tak, aby promowały integrację społeczną i zapewniały spójność wielu usług. W związku z tym wszystkie aplikacje używane na Androidzie 12 lub nowszym muszą obsługiwać najnowszą wersję Unicode Emoji .

Aplikacje, które używają domyślnych emotikonów Androida bez żadnych modyfikacji, podczas działania na Androidzie 12 lub nowszym wykorzystują już najnowszą wersję Unicode Emoji.

Aplikacje ze zmodyfikowanymi emotikonami, również z bibliotek zewnętrznych, podczas działania na Androidzie 12 lub nowszym muszą w pełni obsługiwać najnowszą wersję Unicode. Na spełnienie tego wymogu mają 4 miesiące od opublikowania nowego standardu Unicode Emoji.

Informacje o obsłudze współczesnych emotikonów znajdziesz w tym przewodniku .

Skorzystaj z poniższych przykładów emotikonów, aby sprawdzić, czy aplikacja jest zgodna z najnowszą wersją Unicode:

Przykłady	Wersja Unicode
🫠 🫱🏻‍🫲🏽 🫵🏾	14.0
😶‍🌫️ 👩🏻‍❤️‍👩🏿	13.1
🥲 🧑🏿‍🦲 🐻‍❄️	13.0
🧑‍🦰 🚶‍♀️‍➡️ 👫	12.1
🦩 🫅🏿 👭	12.0

Dla rodzin

Google Play to miejsce, w którym deweloperzy mogą publikować różnego rodzaju wartościowe treści, które są przeznaczone dla całej rodziny. Przed zgłoszeniem aplikacji do programu Dla całej rodziny lub przesłaniem aplikacji skierowanej do dzieci do Sklepu Google Play, musisz się upewnić, że jest ona odpowiednia dla dzieci i zgodna ze stosownymi przepisami.

Dowiedz się więcej o procesie publikowania aplikacji dla rodzin i przejrzyj interaktywną listę kontrolną w Akademii dla deweloperów aplikacji

Tworzenie aplikacji dla dzieci i rodzin

Technologia stała się narzędziem, które zapewnia rodzinie coraz więcej możliwości i rozrywki, dlatego rodzice szukają bezpiecznych treści o wysokiej jakości, które byłyby odpowiednie dla ich dzieci.

Aplikacje mogą być opracowane specjalnie dla dzieci albo po prostu atrakcyjne dla młodszego odbiorcy. W obydwu przypadkach zespół Google Play pomaga deweloperom zapewnić, że aplikacje są bezpieczne dla wszystkich użytkowników, w tym całych rodzin.

Słowo „dziecko” może mieć wiele znaczeń w zależności od regionu i kontekstu. Dlatego ważne jest, by skonsultować się z radcą prawnym i określić zobowiązania oraz ograniczenia wynikające z kierowania treści do użytkowników z określonych kategorii wiekowych. To Ty najlepiej znasz swoje aplikacje, dlatego przy określaniu, czy mogą pojawić się w Sklepie Google i są odpowiednie dla rodzin, polegamy na Twoim osądzie.

Aplikacje przeznaczone dla dzieci muszą uczestniczyć w programie Dla całej rodziny. Jeśli Twoja aplikacja jest skierowana zarówno do dzieci, jak i do starszych odbiorców, nadal możesz uczestniczyć w programie Dla całej rodziny. Wszystkie aplikacje zarejestrowane w tym programie mogą zostać zgłoszone do Programu aplikacji zatwierdzonych przez nauczycieli, jednak nie możemy zagwarantować, że Twoja aplikacja zostanie do niego zakwalifikowana. Jeśli nie chcesz uczestniczyć w programie Dla całej rodziny, nadal obowiązują Cię Zasady dotyczące aplikacji dla rodzin w Google Play (znajdziesz je poniżej), a także pozostałe Zasady programu dla deweloperów w Google Play oraz Umowa dystrybucyjna dla deweloperów.

Wymagania dotyczące Konsoli Play

Docelowi odbiorcy i treści

Przed opublikowaniem aplikacji musisz wskazać jej docelowych odbiorców w sekcji Docelowi odbiorcy i treści w Konsoli Google Play. Aby to zrobić, wybierz grupy wiekowe z listy. Jeśli w aplikacji zamieszczane są obrazy i sformułowania, które mogą zostać uznane za skierowane do dzieci, może to wpłynąć na ocenę deklarowanych docelowych odbiorców przez Google Play – niezależnie od tych określonych w Konsoli Google Play. Google Play zastrzega sobie prawo do sprawdzenia podanych informacji o aplikacji, by określić, czy docelowi odbiorcy zostali właściwie wskazani.

Jeśli wskazanymi odbiorcami docelowymi są tylko osoby dorosłe, ale Google ustali, że ta informacja jest niedokładna, ponieważ aplikacja jest skierowana zarówno do dzieci, jak i do dorosłych, dostępna będzie możliwość jasnego poinformowania użytkowników, że aplikacja nie jest przeznaczona dla dzieci. W tym celu musisz wyrazić zgodę na przypisanie jej etykiety ostrzegawczej.

Więcej niż jedną grupę wiekową docelowych odbiorców aplikacji możesz wybrać tylko wtedy, gdy aplikacja została opracowana z myślą o użytkownikach w różnym wieku. Na przykład aplikacje przeznaczone dla małych dzieci i przedszkolaków powinny mieć tylko grupę wiekową „Do 5 lat”. Jeśli aplikacja jest przeznaczona dla uczniów z określonych klas, musisz wybrać grupę wiekową, która najlepiej do nich pasuje. Przedziały wiekowe, które uwzględniają dorosłych i dzieci, należy uwzględniać tylko wtedy, jeśli aplikacja rzeczywiście została opracowana dla wszystkich grup wiekowych.

Aktualizacje w sekcji Docelowi odbiorcy i treści

Informacje w sekcji Docelowi odbiorcy i treści w Konsoli Google Play możesz aktualizować w dowolnym momencie. Przed opublikowaniem tych informacji w Sklepie Google Play wymagana jest aktualizacja aplikacji. Pamiętaj, że wszelkie zmiany w tej sekcji Konsoli Google Play mogą zostać sprawdzone pod kątem zgodności z zasadami jeszcze przed przesłaniem aktualizacji aplikacji.

Zdecydowanie zalecamy poinformowanie dotychczasowych użytkowników o zmianie grupy wiekowej odbiorców aplikacji lub rozpoczęciu korzystania z reklam albo zakupów w aplikacji. Aby to zrobić, skorzystaj z powiadomień w aplikacji lub sekcji „Nowości” na stronie z informacjami o aplikacji.

Wprowadzanie w błąd przy użyciu Konsoli Play

Fałszywe przedstawianie informacji o aplikacji w Konsoli Play, w tym w sekcji Docelowi odbiorcy i treści, może spowodować jej usunięcie lub zawieszenie, dlatego ważne jest podanie właściwych informacji.

Wymagania dotyczące aplikacji dla rodzin

Jeśli jedną z grup docelowych odbiorców aplikacji są dzieci, musisz spełnić te wymagania. Niezastosowanie się do nich może skutkować usunięciem lub zawieszeniem aplikacji.

1. **Treść aplikacji:** treść aplikacji, do której mają dostęp dzieci, musi być dla nich odpowiednia. Jeśli Twoja aplikacja zawiera treści, które nie są przyjęte za odpowiednie na całym świecie, ale w konkretnym regionie są uznawane za odpowiednie dla niepełnoletnich, może ona być dostępna dla użytkowników w tym regionie (w wybranych regionach), ale nie będzie dostępna w innych.
2. **Funkcje aplikacji:** aplikacja nie może wyłącznie oferować podglądu strony internetowej ani mieć głównie na celu kierowania do strony internetowej bez względu na to, kto jest właścicielem takiej strony.
   - Stale szukamy sposobów na umożliwienie deweloperom aplikacji dla dzieci wprowadzania nowych funkcji. Jeśli interesuje Cię udział w naszym programie pilotażowym dotyczącym zaufanych internetowych aplikacji edukacyjnych, chęć dołączenia do niego możesz zgłosić tutaj .
3. **Odpowiedzi w Konsoli Play:** dokładnie odpowiadaj na pytania na temat aplikacji w Konsoli Play i na bieżąco aktualizuj odpowiedzi, aby odzwierciedlały one zmiany w aplikacji. W kwestionariuszu oceny treści musisz na przykład podać informacje o zawartych w aplikacji elementach interaktywnych, czyli między innymi określić:
   - czy aplikacja umożliwia interakcje lub wymianę informacji między użytkownikami,
   - czy aplikacja udostępnia firmom zewnętrznym informacje podane przez użytkownika,
   - czy aplikacja udostępnia innym fizyczną lokalizację użytkownika.
4. **Reklamy:** jeśli aplikacja wyświetla reklamy dzieciom lub użytkownikom w nieznanym wieku:
   - do wyświetlania reklam takim użytkownikom używaj wyłącznie pakietów SDK do wyświetlania reklam z certyfikatem Google Play ;
   - dopilnuj, żeby reklamy wyświetlane takim użytkownikom nie były oparte na zainteresowaniach (czyli żeby nie były to reklamy kierowane na poszczególnych użytkowników, których cechy określono na podstawie ich zachowań podczas przeglądania internetu) ani remarketingu (czyli żeby nie były to reklamy kierowane na poszczególnych użytkowników na podstawie ich wcześniejszej interakcji z aplikacją lub stroną);
   - dopilnuj, żeby reklamy wyświetlane takim użytkownikom zawierały treści odpowiednie dla tego typu odbiorców;
   - dopilnuj, żeby reklamy wyświetlane takim użytkownikom spełniały wymagania związane z formatem reklamy dla rodzin;
   - zapewnij zgodność ze stosownymi przepisami prawa i standardami branżowymi dotyczącymi wyświetlania reklam dzieciom.
5. **Postępowanie z danymi:** zamieść informację o gromadzeniu przez aplikację (w tym przez używane przez nią interfejsy API i pakiety SDK) wszelkich danych osobowych i wrażliwych o dzieciach. Dane wrażliwe o dzieciach to między innymi dane uwierzytelniające, dane rejestrowane za pomocą mikrofonu i aparatu, dane o urządzeniu, identyfikator Androida oraz dane o korzystaniu z reklam. Musisz też dopilnować, aby aplikacja była zgodna z wymienionymi poniżej sposobami postępowania z danymi:
   - Aplikacje kierowane wyłącznie do dzieci nie mogą przesyłać identyfikatora wyświetlania reklam na urządzeniach z Androidem (AAID), numeru seryjnego karty SIM, numeru seryjnego kompilacji ani identyfikatorów BSSID, MAC, SSID, IMEI czy IMSI.
   - Aplikacje skierowane zarówno do dzieci, jak i do starszych odbiorców nie mogą przekazywać numeru seryjnego karty SIM, numeru seryjnego kompilacji ani identyfikatorów AAID, BSSID, MAC, SSID, IMEI i IMSI dzieci i osób w nieznanym wieku.
   - Nie możesz wyodrębniać numeru telefonu urządzenia z klasy TelephonyManager w interfejsie Android API.
   - Aplikacje skierowane wyłącznie do dzieci nie mogą prosić o dostęp do lokalizacji ani zbierać, wykorzystywać czy przekazywać dokładnej lokalizacji .

- Żądając połączenia Bluetooth, aplikacje muszą używać Menedżera urządzeń towarzyszących , chyba że są przeznaczone na urządzenia z systemem operacyjnym w wersji, która go nie obsługuje.

6. **Interfejsy API i pakiety SDK:** dopilnuj, aby interfejsy API i pakiety SDK były prawidłowo zaimplementowane w aplikacji.
   - Aplikacje skierowane wyłącznie do dzieci nie mogą zawierać żadnych interfejsów API ani pakietów SDK, które nie zostały zatwierdzone do używania w usługach przeznaczonych głównie dla dzieci. Obejmuje to Logowanie przez Google (lub dowolne usługi API Google, które mają dostęp do danych powiązanych z kontem Google), usługi gier Google Play oraz inne usługi API korzystające z protokołu OAuth do uwierzytelniania i autoryzacji.
   - Aplikacje skierowane zarówno do dzieci, jak i starszych odbiorców, nie mogą implementować interfejsów API ani pakietów SDK, które nie zostały zatwierdzone do użytku w usługach skierowanych do dzieci. Są jednak dozwolone, jeśli dostępu do nich chroni neutralny ekran wyboru wieku lub są zaimplementowane w sposób, który nie skutkuje zbieraniem danych o dzieciach. Aplikacje skierowane zarówno do dzieci, jak i do starszych odbiorców nie mogą wymagać od użytkowników logowania się ani dostępu do treści aplikacji za pomocą interfejsu API lub pakietu SDK, który nie został zatwierdzony do użytku w usługach skierowanych do dzieci.

7. **Rzeczywistość rozszerzona (AR):** jeśli aplikacja zawiera sekcje wykorzystujące rzeczywistość rozszerzoną, tuż przed ich uruchomieniem musi się wyświetlić odpowiednie ostrzeżenie. Powinny tam być zawarte te informacje:
   - komunikat informujący o tym, jak ważny jest nadzór rodzicielski;
   - przypomnienie, by zwracać uwagę na zagrożenia w świecie rzeczywistym (np. na otoczenie);
   - Aplikacja nie może wymagać użycia urządzenia, z którego korzystanie nie jest zalecane w przypadku dzieci (takiego jak Daydream czy Oculus).

8. **Aplikacje i funkcje społecznościowe:** jeśli aplikacje pozwalają udostępniać lub wymieniać informacje, musisz dokładnie wyszczególnić te funkcje w kwestionariuszu oceny treści w Konsoli Play.
   - Aplikacje społecznościowe: aplikacje, których głównym celem jest umożliwianie wymiany własnych treści lub komunikowania się z dużymi grupami ludzi. Wszystkie aplikacje społecznościowe, które w grupie odbiorców uwzględniają dzieci, zanim pozwolą dzieciom udostępniać własne treści multimedialne lub informacje, muszą pokazać im przypomnienie przestrzegające przed niebezpieczeństwami związanymi z korzystaniem z internetu i przed pojawiającymi się później w świecie rzeczywistym konsekwencjami interakcji online. Należy również wymagać podjęcia działań przez osoby dorosłe, zanim dzieci będą mogły wymieniać dane osobowe.
   - Funkcje społecznościowe: funkcja społecznościowa to dowolna dodatkowa funkcja aplikacji, która pozwala udostępniać własne treści lub komunikować się z dużymi grupami ludzi. Zanim dowolna aplikacja, która w grupie odbiorców uwzględnia dzieci i oferuje funkcje społecznościowe, pozwoli dzieciom udostępniać własne treści multimedialne lub informacje, musi pokazać im przypomnienie przestrzegające przed niebezpieczeństwami związanymi z korzystaniem z internetu i przed pojawiającymi się później w świecie rzeczywistym konsekwencjami interakcji online. Należy również zapewnić dorosłym sposób zarządzania funkcjami społecznościowymi dzieci, w tym między innymi możliwość włączenia/wyłączenia funkcji społecznościowych lub wybrania różnych poziomów ich działania. Dodatkowo należy wymagać podjęcia działań przez osoby dorosłe przed włączeniem funkcji umożliwiających dzieciom wymianę danych osobowych.
   - Działania podejmowane przez osoby dorosłe to mechanizmy, które pozwalają sprawdzić, czy użytkownik nie jest dzieckiem, i nie zachęcają dziecka do sfałszowania wieku w celu uzyskania dostępu do obszarów aplikacji, które są przeznaczone dla dorosłych (np. podanie przez osobę dorosłą kodu PIN, hasła, daty urodzenia, potwierdzenie adresu e-mail, przesłanie zdjęcia dokumentu tożsamości, karty kredytowej lub numeru ubezpieczenia społecznego).

- Aplikacje społecznościowe, których głównym przeznaczeniem jest rozmowa z osobami, których się nie zna, nie mogą być skierowane do dzieci. Przykłady: aplikacje takie jak Chat Roulette, aplikacje randkowe, otwarte pokoje czatu dla dzieci.

9. **Zgodność z prawem:** dopilnuj, aby aplikacja, w tym używane przez nią interfejsy API i pakiety SDK, była zgodna z amerykańską ustawą o ochronie prywatności dzieci w internecie (Children's Online Privacy and Protection Act, COPPA) , unijnym Ogólnym rozporządzeniem o ochronie danych (RODO) , a także wszystkimi innymi obowiązującymi przepisami i regulacjami prawnymi.

Aby zagwarantować, że platforma Google Play jest bezpiecznym i tolerancyjnym miejscem, stworzyliśmy standardy, które definiują i blokują materiały szkodliwe lub nieodpowiednie dla naszych użytkowników.

- Aplikacje, które w opisie są promowane jako przeznaczone dla dzieci, ale w rzeczywistości ich treści są odpowiednie tylko dla osób dorosłych.
- Aplikacje zawierające interfejsy API, których warunki korzystania zabraniają ich użycia w aplikacjach skierowanych do dzieci.
- Aplikacje w sposób pozytywny przedstawiające spożywanie alkoholu, używanie tytoniu lub substancji kontrolowanych.
- Aplikacje umożliwiające uprawianie realnego lub symulowanego hazardu.
- Aplikacje prezentujące przemoc bądź treści drastyczne lub szokujące, które nie są odpowiednie dla dzieci.
- Aplikacje oferujące serwisy randkowe albo porady seksualne lub małżeńskie.
- Aplikacje zawierające linki do witryn prezentujących treści naruszające Zasady programu dla deweloperów w Google Play.
- Aplikacje, które wyświetlają dzieciom reklamy dla dorosłych (np. prezentujące przemoc, treści erotyczne, hazard). Więcej informacji o zasadach Google Play związanych z reklamami, zakupami w aplikacji i treściami komercyjnymi dla dzieci znajdziesz w zasadach dotyczących reklam odpowiednich dla rodzin i zarabiania na nich.

Program Dla całej rodziny

Aplikacje przeznaczone dla dzieci muszą uczestniczyć w programie Dla całej rodziny. Do programu możesz zgłosić też aplikacje przeznaczone dla wszystkich grup odbiorców, w tym dzieci i całych rodzin.

Aby Twoja aplikacja mogła zostać zaakceptowana w programie, musisz przestrzegać Zasad programu dla deweloperów w Google Play oraz Umowy dystrybucyjnej dla deweloperów . Oprócz tego aplikacja musi być zgodna ze wszystkimi Zasadami dotyczącymi aplikacji dla rodzin oraz spełniać wymagania programu Dla całej rodziny.

Więcej informacji o procesie zgłaszania aplikacji do programu znajdziesz tutaj .

Kwalifikacja do programu

Wszystkie aplikacje uczestniczące w programie Dla całej rodziny i zawarte w nich treści (w tym treści reklam) muszą być odpowiednie dla dzieci (muszą mieć ocenę Dla wszystkich lub Dla wszystkich od 10 lat w systemie ESRB albo równoważną w innym systemie ocen) i muszą korzystać wyłącznie z pakietów SDK reklam z certyfikatem Google Play . Aplikacje przyjęte do programu Dla całej rodziny muszą zachować zgodność ze wszystkimi jego wymaganiami. Google Play może odrzucić, usunąć lub zawiesić dowolną aplikację, którą uzna za niezgodną z zasadami programu Dla całej rodziny.

Here are some examples of common apps that are ineligible for the program:

- Aplikacje, które mają ocenę Dla wszystkich w systemie ESRB, ale zawierają reklamy promujące hazard.
- Aplikacje dla rodziców i opiekunów (np. służące do monitorowania karmienia piersią czy zawierające poradniki na temat prawidłowego rozwoju dziecka).

- Poradniki dla rodziców i aplikacje do zarządzania urządzeniem, które są przeznaczone wyłącznie dla rodziców lub opiekunów.

Kategorie

W przypadku przyjęcia do programu Dla całej rodziny możesz wybrać drugą kategorię związaną z programem, która także opisuje aplikację. Oto kategorie aplikacji dostępne w programie Dla całej rodziny:

Akcja i przygoda: aplikacje i gry pełne akcji, w tym proste wyścigi, przygody w świecie baśni i inne aplikacje oraz gry, które zostały opracowane z myślą o wzbudzaniu ekscytacji.

Gry logiczne: gry wymagające myślenia, w tym łamigłówki, układanki, quizy i inne gry, które stanowią wyzwanie dla pamięci lub intelektu bądź opierają się na umiejętności logicznego myślenia.

Kreatywność: aplikacje i gry pobudzające kreatywność, które umożliwiają np. rysowanie, malowanie, programowanie lub budowanie różnych rzeczy.

Edukacja: aplikacje i gry opracowane pod okiem ekspertów (pedagogów, specjalistów ds. nauczania czy naukowców), które mają za cel promowanie uczenia się, w tym zdobywania wiedzy, nabywania umiejętności społeczno-emocjonalnych lub fizycznych czy rozwijania kreatywnego myślenia, a także pomagają w zdobyciu elementarnych umiejętności życiowych oraz zachęcają do krytycznego myślenia i rozwiązywania problemów.

Muzyka i film: aplikacje i gry zawierające komponent muzyczny lub filmowy, od aplikacji symulujących instrumenty po takie, które dostarczają muzyczne treści audio i wideo.

Zabawa w udawanie: aplikacje i gry, w których użytkownik może wcielać się w różne role, np. udawać, że jest kucharzem, opiekunem, księciem/księżniczką, strażakiem, policjantem lub postacią fikcyjną.

Reklamy i zarabianie

W przypadku zarabiania w Play na aplikacji skierowanej do dzieci należy dopilnować, aby była ona zgodna z zasadami dotyczącymi zarabiania i reklam odpowiednich dla rodzin.

Zawarte poniżej zasady obowiązują w przypadku wszystkich elementów generujących przychody i reklam, w tym wzajemnych promocji (zarówno promujących Twoje aplikacje, jak i te autorstwa innych deweloperów), ofert zakupu w aplikacji oraz innych treści komercyjnych (np. płatnego lokowania produktu). Wszystkie elementy do generowania przychodu i reklamy w tych aplikacjach muszą być zgodne ze wszystkimi obowiązującymi przepisami (w tym ze wszelkimi wytycznymi branżowymi i regulacjami wewnętrznymi).

Google Play zastrzega sobie prawo do odrzucenia, usunięcia lub zawieszenia aplikacji, która stosuje zbyt agresywne praktyki promocyjne.

Wymagania związane z formatem

Opcje generowania przychodu i reklamy w aplikacji nie mogą zawierać treści wprowadzających w błąd ani nie mogą być zaprojektowane w sposób, który będzie powodował niezamierzone klikanie ich przez dzieci. Zabronione są:

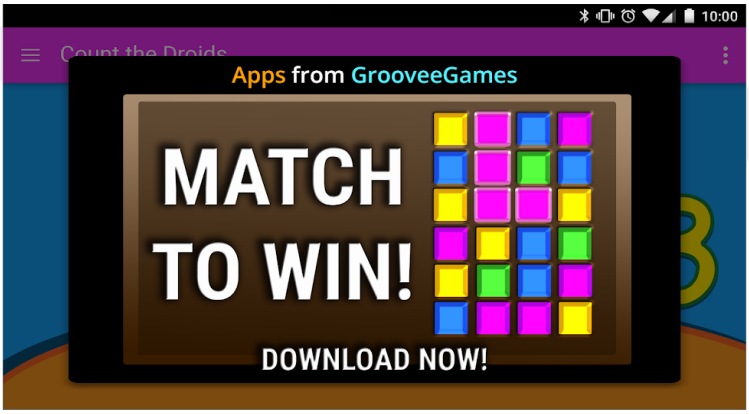
- uciążliwe opcje generowania przychodu i reklamy, w tym zajmujące pełny ekran lub zakłócające normalne działanie, które nie informują w jasny sposób, jak je zamknąć (np. ściany reklam);
- opcje generowania przychodu i reklamy, które zakłócają zwykłe korzystanie z aplikacji lub gry i których nie można zamknąć po 5 sekundach.
- Opcje generowania przychodu i reklamy, które nie zakłócają normalnego korzystania z aplikacji lub gry, mogą być wyświetlane przez ponad 5 sekund – np. treści wideo z reklamami zintegrowanymi;
- opcje generowania przychodu lub reklamy pełnoekranowe w aplikacji wyświetlane tuż po jej uruchomieniu;

- umieszczanie wielu reklam na stronie (np. stosowanie banerów reklamowych, które wyświetlają wiele ofert w jednym miejscu docelowym, lub wyświetlanie więcej niż 1 baneru lub reklamy wideo);
- opcje generowania przychodu lub reklamy w aplikacji, których nie można łatwo odróżnić od treści aplikacji;
- szokujące lub oddziałujące na emocje taktyki zachęcania do wyświetlenia reklamy lub zakupu w aplikacji;
- brak rozróżnienia między wirtualnymi środkami w grze a rzeczywistymi pieniędzmi, które można przeznaczyć na zakupy w aplikacji.

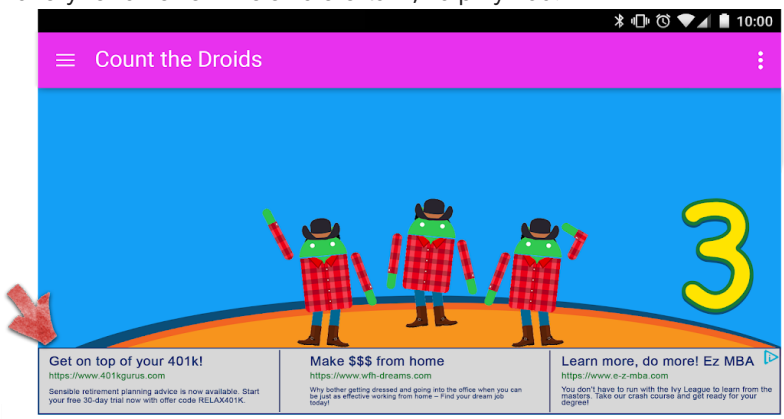
Aby zagwarantować, że platforma Google Play jest bezpiecznym i tolerancyjnym miejscem, stworzyliśmy standardy, które definiują i blokują materiały szkodliwe lub nieodpowiednie dla naszych użytkowników.

- Opcje generowania przychodu i reklamy, które przesuwają się tak, aby nie można było kliknąć ich palcem w celu zamknięcia.
- Opcje generowania przychodu i reklamy, które nie umożliwiają zamknięcia ich po pięciu (5) sekundach, na przykład:

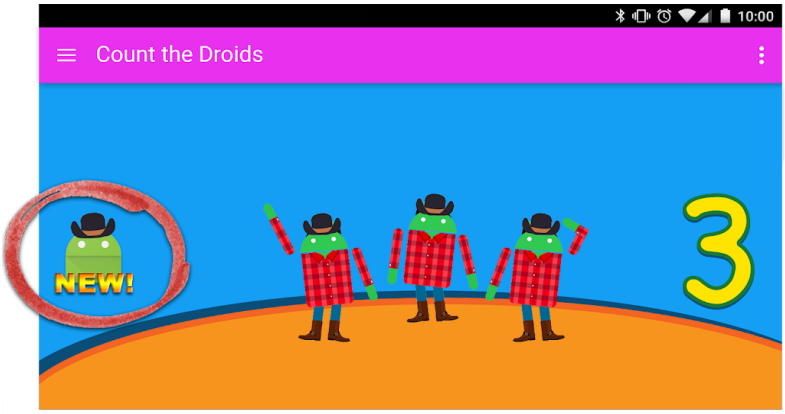
- Opcje generowania przychodu i reklamy, które zajmują większość ekranu lub cały ekran urządzenia i uniemożliwiają użytkownikowi ich zamknięcie, na przykład:



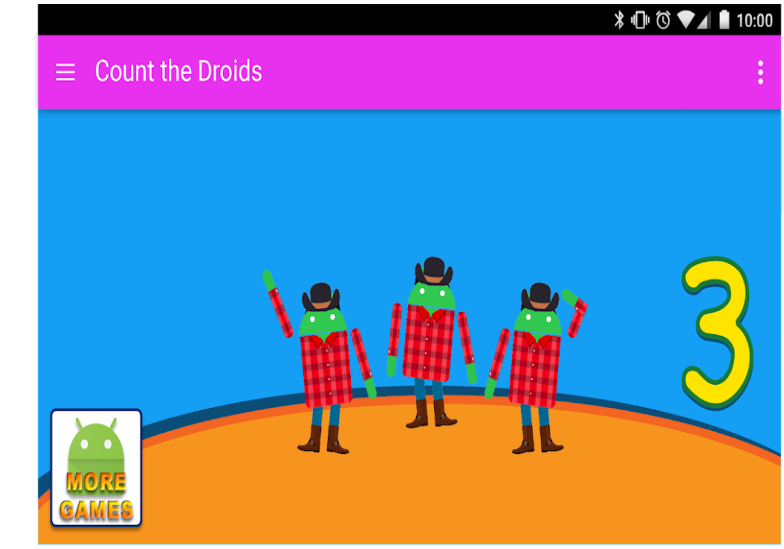
- Banery reklamowe z wieloma ofertami, na przykład:



- Opcje generowania przychodu i reklamy, które można pomylić z treścią aplikacji, na przykład:



- Przyciski, reklamy lub inne opcje generowania przychodu, które promują inne aplikacje w Sklepie Google Play, ale nie można ich odróżnić od treści aplikacji. Przykład:



Oto kilka przykładów nieodpowiednich treści reklam, których nie należy wyświetlać dzieciom:

- **nieodpowiednie treści multimedialne:** reklamy seriali, filmów, albumów muzycznych i innych produktów multimedialnych nieodpowiednich dla dzieci;
- **nieodpowiednie gry wideo i oprogramowanie do pobrania:** reklamy programów do pobrania i elektronicznych gier wideo nieodpowiednich dla dzieci;
- **substancje kontrolowane lub szkodliwe:** reklamy alkoholu, tytoniu, substancji kontrolowanych lub dowolnych innych szkodliwych substancji;

- **hazard:** reklamy symulowanego hazardu, promocyjne konkursy i loterie (nawet takie, w których można uczestniczyć bezpłatnie);
- **treści dla dorosłych i treści o charakterze erotycznym:** reklamy zawierające treści erotyczne, dwuznaczne i przeznaczone dla dorosłych;
- **randki i związki:** reklamy serwisów randkowych lub witryn dla dorosłych szukających związku;
- **przemoc:** reklamy prezentujące przemoc i treści drastyczne, nieodpowiednie dla dzieci.

Pakiety SDK do wyświetlania reklam

Jeśli wyświetlasz w aplikacji reklamy, a docelowi odbiorcy to wyłącznie dzieci, musisz używać samodzielnie certyfikowanych pakietów SDK do wyświetlania reklam odpowiednich dla rodzin. Jeśli aplikacja jest skierowana nie tylko do dzieci, ale też i do starszych użytkowników, zaimplementuj mechanizm sprawdzania wieku, np. neutralny ekran wyboru wieku. Dodatkowo dopilnuj, żeby reklamy wyświetlane dzieciom pochodziły wyłącznie z samodzielnie certyfikowanych pakietów SDK do wyświetlania reklam odpowiednich dla rodzin. Aplikacje uczestniczące w programie Dla całej rodziny mogą korzystać wyłącznie z samodzielnie certyfikowanych pakietów SDK do wyświetlania reklam.

Więcej informacji o tych wymaganiach i aktualną listę samodzielnie certyfikowanych pakietów SDK znajdziesz na stronie z zasadami Programu samodzielnej certyfikacji pakietów SDK do wyświetlania reklam odpowiednich dla rodzin.

Jeśli korzystasz z AdMob, szczegółowe informacje o dostępnych usługach znajdziesz w Centrum pomocy AdMob.

To Ty odpowiadasz za to, żeby aplikacja spełniała wszystkie wymagania związane z reklamami, zakupami w aplikacji i treściami komercyjnymi. Aby dowiedzieć się więcej o polityce treści i metodach stosowanych przez dostawcę pakietu SDK do wyświetlania reklam, skontaktuj się z nim.

Zakupy w aplikacji

Przed dokonaniem zakupu w aplikacji uczestniczącej w programie Dla całej rodziny, Google Play każdorazowo przeprowadza uwierzytelnienie użytkownika. Dzięki temu mamy pewność, że zakup zatwierdza osoba odpowiedzialna finansowo, a nie dziecko.

Enforcement

Avoiding a policy violation is always better than managing one, but when violations do occur, we're committed to ensuring developers understand how they can bring their app into compliance. Please let us know if you see any violations or have any questions about managing a violation.

Zakres zasad

Nasze zasady obejmują wszystkie materiały, które Twoja aplikacja wyświetla lub udostępnia w postaci linków, w tym reklamy pokazywane użytkownikom oraz treści użytkowników umieszczone w aplikacji lub dostępne w niej przez linki. Obowiązują one także w odniesieniu do wszystkich treści pochodzących z konta dewelopera, które są wyświetlane publicznie w Google Play – w tym nazwy dewelopera oraz strony docelowej w jego publicznej witrynie.

Zabraniamy publikowania aplikacji, które umożliwiają użytkownikom instalowanie innych aplikacji na urządzeniach. W przypadku aplikacji, które umożliwiają dostęp do innych aplikacji, gier lub programów bez instalacji, w tym funkcji i usług zapewnianych przez firmy zewnętrzne, musisz dopilnować, by wszystkie udostępniane w ten sposób treści były zgodne ze wszystkimi zasadami Google Play – mogą one podlegać dodatkowej weryfikacji.

Definicje terminów użytych w tych zasadach są takie same jak w Umowie dystrybucyjnej dla deweloperów. Oprócz zachowania zgodności z tymi zasadami i Umową dystrybucyjną dla deweloperów musisz ocenić zawartość swojej aplikacji zgodnie z naszymi Wytycznymi dotyczącymi oceny treści.

Zabraniamy publikowania aplikacji i treści w aplikacjach, które niekorzystnie wpływają na zaufanie użytkowników do ekosystemu Google Play. Decydując, czy aplikacja powinna być udostępniona w Sklepie Google Play czy z niego usunięta, bierzemy pod uwagę wiele czynników, na przykład potencjalnie szkodliwe działanie czy wysokie ryzyko nadużycia. Ryzyko nadużycia określamy na podstawie wielu elementów, takich jak skargi na aplikację lub dewelopera, dostępne publicznie informacje, wcześniejsze naruszenia, opinie użytkowników oraz wykorzystanie popularnych marek, postaci i innych zasobów.

Jak działa Google Play Protect

Google Play Protect sprawdza aplikacje, gdy je instalujesz. Oprócz tego okresowo skanuje urządzenie. Jeśli znajdzie potencjalnie szkodliwą aplikację, może:

- wysłać powiadomienie – aby usunąć aplikację, kliknij powiadomienie, a potem Odinstaluj;
- wyłączyć aplikację, dopóki jej nie odinstalujesz;
- automatycznie usunąć aplikację – w większości przypadków po wykryciu szkodliwej aplikacji zobaczysz powiadomienie, że została ona usunięta.

Jak działa ochrona przed złośliwym oprogramowaniem

Aby chronić Cię przed złośliwym oprogramowaniem innych firm, adresami URL i innymi problemami związanymi z bezpieczeństwem, Google może otrzymywać takie informacje:

- połączenia sieciowe urządzenia,
- potencjalnie szkodliwe adresy URL,
- system operacyjny i aplikacje zainstalowane na urządzeniu przez Google Play lub z innych źródeł.

Jeśli dana aplikacja lub URL są potencjalnie niebezpieczne, możesz zobaczyć ostrzeżenie od Google. Aplikacja lub URL mogą zostać usunięte lub zablokowane przez Google, jeśli będziemy mieli pewność, że są szkodliwe dla urządzeń, danych lub użytkowników.

Możesz wyłączyć niektóre z tych zabezpieczeń w ustawieniach urządzenia. Nadal jednak możemy otrzymywać informacje o aplikacjach instalowanych z Google Play, a aplikacje instalowane z innych źródeł mogą być wciąż sprawdzane pod kątem problemów z zabezpieczeniami – informacje na ten temat nie będą przesyłane do Google.

Jak działają alerty o prywatności

Google Play Protect wyśle alert, jeśli aplikacja zostanie usunięta ze Sklepu Google Play ze względu na możliwość dostępu do Twoich danych osobowych. Będziesz mieć możliwość odinstalowania aplikacji.

Proces egzekwowania zasad

Jeśli Twoja aplikacja narusza nasze zasady, podejmiemy odpowiednie działania opisane poniżej.Poza tym dostaniesz od nas e-maila z informacją o podjętym działaniu oraz instrukcją odwołania się od tej decyzji, jeśli uważasz, że popełniliśmy błąd.

Powiadomienia o usunięciu lub powiadomienia administracyjne mogą nie wskazywać każdego z naruszeń zasad występujących w związku z aplikacją lub grupą aplikacji. Deweloperzy muszą rozwiązać problemy związane z naruszeniami i dokładnie sprawdzić, czy pozostała część aplikacji jest w pełni zgodna z naszymi zasadami. Jeśli nie rozwiążesz problemu niezgodności z zasadami we wszystkich aplikacjach, możemy podjąć dalsze działania mające na celu wyegzekwowanie stosowania się do naszych zasad.

Powtarzające się lub poważne naruszenia tych zasad (np. złośliwe oprogramowanie, oszustwo lub aplikacje mogące uszkodzić urządzenie lub wyrządzić inne szkody użytkownikowi) lub Umowy dystrybucyjnej dla deweloperów skutkują zamknięciem danego konta dewelopera w Google Play lub kont z nim powiązanych.

Działania związane z egzekwowaniem zasad

Różne działania związane z egzekwowaniem zasad mogą mieć różny wpływ na Twoją aplikację.W tej sekcji opisujemy różne działania, jakie może podjąć Google Play, oraz ich wpływ na aplikację lub konto dewelopera w Google Play.Te informacje omówiliśmy również w tym filmie.

Odrzucenie

- Nowa aplikacja lub aktualizacja aplikacji przesłana do sprawdzenia nie będzie dostępna w Google Play.
- Jeśli odrzuciliśmy aktualizację już dostępnej aplikacji, wersja opublikowana przed tą aktualizacją pozostanie dostępna w Google Play.
- Odrzucenia nie mają wpływu na dostęp do dotychczas zebranych danych takich jak instalacje, statystyki czy oceny odrzuconej aplikacji.
- Odrzucenia nie mają wpływu na opinię o Twoim koncie dewelopera w Google Play.

Uwaga: nie próbuj ponownie przesłać odrzuconej aplikacji, dopóki nie usuniesz wszystkich naruszeń zasad.

Usunięcie

- Aplikacja wraz z jej wcześniejszymi wersjami zostanie usunięta z Google Play i nie będzie dłużej dostępna do pobrania dla użytkowników.
- Ponieważ aplikacja zostanie usunięta, użytkownicy nie będą mogli zobaczyć strony z informacjami o niej, liczby instalacji, statystyk ani ocen. Te informacje zostaną przywrócone po przesłaniu zgodnej z zasadami aktualizacji usuniętej aplikacji.
- Użytkownicy mogą nie mieć możliwości robienia zakupów w aplikacji ani korzystania z funkcji rozliczeń w aplikacji do czasu zatwierdzenia jej przez Google Play.
- Usunięcie nie wpływa od razu na opinię o Twoim koncie dewelopera w Google Play, jednak wielokrotne usunięcia mogą spowodować jego zawieszenie.

Uwaga: nie próbuj ponownie publikować usuniętej aplikacji, dopóki nie usuniesz wszystkich naruszeń zasad.

Zawieszenie

- Aplikacja wraz z jej wcześniejszymi wersjami zostanie usunięta z Google Play i nie będzie dłużej dostępna do pobrania dla użytkowników.
- Zawieszenie może nastąpić w wyniku rażącego lub wielokrotnego naruszenia zasad albo wielokrotnego odrzucania lub usuwania aplikacji.
- Ponieważ aplikacja zostanie zawieszona, użytkownicy nie będą mogli zobaczyć strony z informacjami o niej, liczby dotychczasowych instalacji, statystyk ani ocen.Te informacje zostaną przywrócone po przesłaniu aktualizacji zgodnej z zasadami.
- Nie możesz dłużej używać tego samego pliku APK ani pakietu aplikacji.
- Użytkownicy nie będą mieli możliwości robienia zakupów w aplikacji ani korzystania z funkcji rozliczeń w aplikacji do czasu zatwierdzenia jej przez Google Play.
- Zawieszenie ma niekorzystny wpływ na opinię o koncie dewelopera w Google Play.Kolejne zdarzenia tego typu mogą spowodować zamknięcie konta danego dewelopera w Google Play i jego kont powiązanych.

Uwaga: nie próbuj ponownie publikować zawieszonej aplikacji, dopóki Google Play nie poinformuje Cię, że możesz to zrobić.

Ograniczona widoczność

- Możliwość znalezienia Twojej aplikacji w Google Play zostanie ograniczona. Twoja aplikacja pozostanie dostępna w Google Play – będą mieć do niej dostęp użytkownicy dysponujący bezpośrednim linkiem do strony z informacjami o aplikacji w Google Play.
- Nadanie aplikacji stanu ograniczonej widoczności nie ma wpływu na opinię o Twoim koncie dewelopera w Google Play.
- Nadanie aplikacji stanu ograniczonej widoczności nie ma wpływu na możliwość wyświetlania dotychczasowych informacji o aplikacji, liczby instalacji, statystyk czy ocen.

Wybrane regiony

- Aplikację można pobierać tylko z Google Play w określonych regionach.
- Użytkownicy z innych regionów nie będą mogli znaleźć aplikacji w Sklepie Play.
- Użytkownicy, którzy zainstalowali aplikację wcześniej i nadal z niej korzystają na swoich urządzeniach, nie będą otrzymywać aktualizacji.
- Ograniczenie dostępności aplikacji według regionu nie wpływa na opinię o Twoim koncie dewelopera w Google Play.

Zamknięcie konta

- W przypadku zamknięcia Twojego konta dewelopera wszystkie aplikacje z Twojego katalogu zostaną usunięte z Google Play i nie będziesz już mieć możliwości publikowania nowych aplikacji. Wszystkie powiązane konta dewelopera w Google Play również zostaną trwale zawieszone.
- Wielokrotne zawieszenia lub zawieszenia wynikające z rażącego naruszenia zasad również mogą spowodować zamknięcie konta w Konsoli Play.
- Ponieważ aplikacje powiązane z zamkniętym kontem zostaną usunięte, użytkownicy nie będą mogli wyświetlić informacji o nich, ich liczby dotychczasowych instalacji, statystyk ani ocen.

Uwaga: każde nowe konto, które spróbujesz otworzyć, również zostanie zamknięte (bez zwrotu opłaty za rejestrację dewelopera) – nie próbuj rejestrować w Konsoli Play nowego konta, jeśli inne Twoje konto zostało zamknięte.

Konta nieaktywne

Konta nieaktywne to konta deweloperów, które zostały porzucone i nie są już używane. Zgodnie z Umową dystrybucyjną dla deweloperów tego typu konta są niepożądane.

Konta deweloperów w Google Play są przeznaczone dla aktywnych deweloperów, którzy publikują aplikacje i na bieżąco je obsługują. Aby zapobiec nadużyciom, regularnie zamykamy konta, które są nieaktywne, nieużywane lub nie są regularnie wykorzystywane, np. na potrzeby publikowania i aktualizowania aplikacji, sprawdzania statystyk czy zarządzania informacjami o aplikacji.

Zamknięcie nieaktywnego konta powoduje usunięcie go wraz z powiązanymi z nim danymi. Opłata rejestracyjna nie zostanie zwrócona. Przed zamknięciem Twojego nieaktywnego konta powiadomimy Cię, korzystając z podanych informacji kontaktowych.

Jeśli zamkniemy Twoje nieaktywne konto, a w przyszłości zdecydujesz się na publikowanie treści w Google Play, nadal będziesz mieć możliwość utworzenia nowego konta. Nie będziesz jednak w stanie ponownie aktywować swojego konta, a poprzednie aplikacje i dane nie będą dostępne na nowym koncie.

Przypadki naruszenia zasad i ich zgłaszanie

Odwołanie od działań związanych z egzekwowaniem zasad

Przywracamy aplikacje w przypadku popełnienia błędu – jeśli okaże się, że aplikacja nie narusza Zasad programu Google Play ani Umowy dystrybucyjnej dla deweloperów. Jeśli po uważnym przeczytaniu zasad uznasz, że nasza decyzja mogła być błędna, możesz się od niej odwołać, postępując zgodnie z instrukcjami podanymi w e-mailu z powiadomieniem o naszym działaniu.

Dodatkowe materiały

Jeśli potrzebujesz więcej informacji na temat jakiegoś działania związanego z egzekwowaniem zasad lub oceny/komentarza użytkownika, możesz skorzystać z tych materiałów lub skontaktować się z nami przez Centrum pomocy Google Play. Nie możemy zaproponować w tym zakresie żadnej pomocy prawnej. W takich sprawach skontaktuj się z radcą prawnym.

- Weryfikowanie aplikacji
- Jak zgłosić naruszenie zasad
- Kontakt z Google Play w sprawie usunięcia konta lub aplikacji
- Wyraźne ostrzeżenia
- Zgłaszanie nieodpowiednich aplikacji i komentarzy
- Moja aplikacja została usunięta z Google Play
- Zamykanie kont dewelopera w Google Play

Wymagania dotyczące Konsoli Play

Chcemy, żeby Sklep Google Play był bezpiecznym i inspirującym miejscem dla naszych użytkowników oraz wzbogacającym środowiskiem dla deweloperów aplikacji. Zależy nam na tym, żeby proces udostępniania aplikacji użytkownikom przebiegał bez żadnych problemów.

Naruszenie zasad może spowolnić sprawdzanie aplikacji lub spowodować jej odrzucenie. Aby uniknąć takich problemów, podczas przesyłania informacji w Konsoli Play pamiętaj o opisanych poniżej kwestiach.

Przed przesłaniem aplikacji:

- Upewnij się, że wszystkie informacje o aplikacji i jej metadane są dokładne.
- Sprawdź, czy Twoje informacje kontaktowe są aktualne.
- Prześlij politykę prywatności obowiązującą w Twojej aplikacji i podaj wymagane informacje w sekcji **Bezpieczeństwo danych**.
- Wskaż aktywne konto demonstracyjne wraz z danymi logowania i podaj wszystkie informacje potrzebne do sprawdzenia aplikacji (login i hasło, kod QR itp.).

Tak jak zawsze zadbaj o to, żeby Twoja aplikacja była stabilna, elastyczna i interesująca dla użytkowników. Wszystkie elementy wchodzące w jej skład (np. sieci reklamowe, usługi analityczne czy zewnętrzne pakiety SDK) muszą być zgodne z Zasadami programu dla deweloperów w Google Play. Jeśli z Twojej aplikacji mogą korzystać także dzieci, upewnij się, że nie narusza ona zasad dotyczących aplikacji dla rodzin .

Pamiętaj, że Twoja aplikacja musi być w pełni zgodna z Umową dystrybucyjną dla deweloperów i wszystkimi Zasadami programu dla deweloperów .

Developer Distribution Agreement

Potrzebujesz dodatkowej pomocy?

Wykonaj te czynności:

Kontakt z nami
Przekaż więcej informacji, byśmy mogli Ci pomóc