Fejlesztői programszabályzat

(ellenkező megjegyzés hiányában 2024. október 30-tól hatályos)

Alakítsuk ki a világ legmegbízhatóbb alkalmazás- és játékforrását

Az Ön újító szándéka a közös sikerünk kulcsa, ám az újító szándék felelősséggel is jár. A Fejlesztői programszabályzat és a Fejlesztői terjesztési megállapodás segít abban, hogy közösen továbbra is a leginnovatívabb és legmegbízhatóbb alkalmazásokat kínálhassuk több mint egymilliárd embernek a Google Playen. Kérjük, olvassa el alábbi szabályzatunkat.

Korlátozott tartalom

Mindennap világszerte használják a Google Playt alkalmazások és játékok keresésére. Alkalmazás beküldése előtt tegye fel magának a kérdést, hogy alkalmazása megfelel-e a Google Play és a helyi jogszabályok előírásainak.

Gyermekek veszélyeztetése

Azokat az alkalmazásokat, amelyek nem tiltják meg a felhasználóknak a gyermekek kizsákmányolását vagy a gyermekekkel való visszaélést elősegítő tartalom létrehozását, feltöltését vagy terjesztését, a Google Playről való azonnali eltávolítás terhe sújtja. Ideértendő a gyermekekkel történő szexuális visszaéléssel kapcsolatos bármilyen anyag. Ha a Google valamelyik termékében olyan tartalmat találsz, amely vélhetően gyermekek kizsákmányolásának minősül, jelentsd be a **Visszaélés bejelentése** elemre kattintva. Ha hasonló tartalmat találsz máshol az interneten, fordulj közvetlenül az országod illetékes hatóságához .

Tiltjuk a gyermekeket veszélyeztető alkalmazások használatát. Idetartozik többek között az olyan alkalmazások használata, amelyek előmozdítják a gyermekekkel szembeni ragadozó viselkedést, így például:

- gyermekeket célzó, nem helyénvaló interakció (például tapogatás vagy simogatás);
- gyermekmolesztálás (például internetes barátkozás gyermekkel szexuális kapcsolat internetes vagy nem internetes elősegítése érdekében és/vagy szexuális tartalmú képek cseréje a gyermekkel);
- kiskorúak szexuális ábrázolása (például olyan képek, amelyek gyermekekkel történő szexuális visszaélést ábrázolnak, bátorítanak vagy népszerűsítenek, illetve gyermekek olyan módon történő ábrázolása, amely gyermekek szexuális kizsákmányolását eredményezheti);
- szexuális tartalmú internetes zsarolás (például gyermek megfélemlítése vagy megzsarolása az intim képeihez történő valós vagy állítólagos hozzáférés használatával);
- gyermekkereskedelem (például gyermekek hirdetése vagy felkínálása kereskedelmi célú szexuális kizsákmányolás céljából).

Ilyen típusú tartalmak esetén megtesszük a szükséges intézkedéseket, például jelentjük az esetet az egyesült államokbeli Eltűnt és Kizsákmányolt Gyermekek Nemzeti Központja (NCMEC) szervezetnek, ha olyan tartalom jut a tudomásunkra, amelyben gyermekekkel történő szexuális visszaéléssel kapcsolatos anyag fordul elő. Ha úgy véled, hogy bántalmazás, kizsákmányolás vagy emberkereskedelem veszélyének van kitéve egy gyermek, vagy ezek valamelyikét követték el ellene, fordulj a helyi rendészeti szervekhez, továbbá fordulj a gyermekek biztonságával foglalkozó, itt felsorolt szervezetek valamelyikéhez.

Emellett nem engedélyezettek a gyermekek számára vonzó, de felnőtteknek szóló témákat tartalmazó alkalmazások sem, beleértve, de nem kizárólagosan a következőket:

- a túlzottan erőszakos, vért és vérontást tartalmazó alkalmazások;

- a kártékony vagy veszélyes tevékenységeket bemutató vagy népszerűsítő alkalmazások.

Nem engedélyezünk továbbá olyan alkalmazásokat, amelyek a negatív test- vagy önképet népszerűsítik – például amelyek szórakoztatási célból plasztikai sebészetet, fogyást vagy emberek fizikai megjelenését érintő más kozmetikai korrekciókat mutatnak be.

Nem helyénvaló tartalom

A Google Play biztonságos és tiszteletteljes platformként való megőrzése érdekében létrehoztuk a felhasználók számára kártékony vagy kifogásolható tartalmak meghatározását és tiltását részletező irányelveket.

Szexuális tartalom és káromkodás

Nem engedélyezünk olyan alkalmazásokat, amelyekben szexuális tartalom (például pornográfia) vagy káromkodás szerepel, illetve olyan tartalmat vagy szolgáltatást foglalnak magukba vagy népszerűsítenek, amelynek célja szexuális vágyak kielégítése. Nem engedélyezünk olyan alkalmazásokat vagy alkalmazástartalmakat, amelyek vélhetően szexuális tevékenységet ellentételezésért kínáló szolgáltatásokat reklámoznak vagy nyújtanak. Nem engedélyezünk olyan alkalmazásokat, amelyek szexuálisan ragadozó viselkedéshez kapcsolódó tartalmat tartalmaznak vagy népszerűsítenek, illetve nem kölcsönös beleegyezésen alapuló szexuális tartalmat terjesztenek. Meztelenséget bemutató tartalom abban az esetben megengedhető, ha elsősorban oktatási, ismeretterjesztő, tudományos vagy művészi célzatú, és nem indokolatlan.

A katalógusalkalmazások – az olyan alkalmazások, amelyek tágabb tartalomkatalógus részeként sorolnak fel könyv-/videócímeket – terjeszthetnek szexuális tartalmú könyveket (e-könyveket és hangoskönyveket is) vagy videókat, feltéve ha teljesülnek a következő követelmények:

- A szexuális tartalmú könyvek/videók az alkalmazás teljes katalógusának elhanyagolható részét teszik ki.
- Az alkalmazás nem népszerűsít aktívan olyan könyvet/videót, amelyben szexuális tartalom szerepel. A szóban forgó tételek így is megjelenhetnek a felhasználói előzmények alapján adott javaslatokban vagy általános árpromóciók során.
- Az alkalmazás nem terjeszt olyan könyvet/videót, amelyben gyermekeket veszélyeztető tartalom, pornó vagy a vonatkozó jogszabályok értelmében illegálisnak minősülő más szexuális tartalom szerepel.
- Az alkalmazás a szexuális tartalmú könyvekhez/videókhoz való hozzáférés korlátozásával védelmet nyújt a kiskorúaknak.

Ha az alkalmazásban olyan tartalom található, amely sérti ezt az irányelvet, ám az adott tartalom megfelelőnek minősül egy adott régióban, a régió felhasználói hozzáférhetnek az alkalmazáshoz, de más régiók felhasználóinak továbbra sem áll majd rendelkezésére.

Néhány példa a gyakori irányelvsértésekre:

- Erotikus meztelenség vagy szexre utaló pózok ábrázolása, amelyekben az alany meztelen, elhomályosított, illetve nagyon kevés ruhát visel, és/vagy a ruházat nem lenne elfogadható megfelelő nyilvános környezetben.
- Szexuális tevékenységek és szexre utaló pózok ábrázolása, animációként vagy illusztrációként való megjelenítése, testrészek szexuális jellegű ábrázolása.
- Olyan tartalmak, amelyek szexuális segédeszközöket, szexuális útmutatást, illegális szexuális témákat és fétiseket mutatnak be, vagy ilyen funkciókkal rendelkeznek.
- Erkölcstelen vagy profán tartalmak – például káromkodás, sértegetés, szókimondó szöveg, felnőtteknek szóló vagy szexuális jellegű kulcsszavak az áruházi adatlapon vagy az alkalmazásban.
- Állatokkal folytatott szexuális tevékenységet ábrázoló, leíró vagy bátorító tartalom.

- Olyan alkalmazások, amelyek szexhez kapcsolódó szórakozást, escortszolgáltatásokat vagy egyéb, vélhetően szexuális tevékenységet ellentételezésért kínáló szolgáltatásokat reklámoznak vagy kérnek, beleértve, de nem kizárólagosan az olyan megállapodásokat, amelyekben az egyik féltől elvárják, hogy pénzt, ajándékokat vagy anyagi támogatást biztosítson a másik félnek (ilyenek például az eltartotti, „sugar" kapcsolatok).
- Alkalmazások, amelyek személyeket degradálnak vagy tárgyiasítanak; például olyan alkalmazások, amelyek emberek levetkőztetését vagy a ruhájukon való átlátást ígérik, még akkor is, ha ugratásként vagy szórakoztató alkalmazásként vannak feltüntetve.
- Olyan tartalom vagy viselkedés, amely szexuális módon megkísérel embereket megfenyegetni vagy kihasználni, úgymint lesifotók, rejtett kamerás felvételek, nem beleegyezésen alapuló, deepfake-kel vagy hasonló technológiával készült szexuális tartalmak vagy zaklató tartalmak.

Gyűlöletkeltés

Nem engedélyezünk olyan alkalmazásokat, amelyek az erőszakot népszerűsítik, egyének vagy csoportok ellen gyűlöletet keltenek faji vagy etnikai származás, vallás, fogyatékosság, életkor, nemzetiség, veterán státusz, szexuális beállítottság, nem, nemi identitás, kaszt, bevándorlási státusz vagy bármely más, szisztematikus diszkriminációval vagy kirekesztéssel kapcsolatos jellemző miatt.

A nácikhoz kapcsolódó EDSA (Educational, Documentary, Scientific, or Artistic; azaz ismeretterjesztő, oktatási, tudományos vagy művészeti) jellegű tartalmakkal rendelkező alkalmazásokat egyes országokban a helyi jogszabályoknak és rendelkezéseknek megfelelően tilthatjuk.

Néhány példa a gyakori irányelvsértésekre:

- Olyan tartalom vagy beszéd, amelynek célja annak bizonyítása, hogy valamelyik védett csoport nem számít embernek, alsóbbrendű vagy gyűlölendő.
- Olyan alkalmazások, amelyek tartalma valamely védett csoportot negatív jellemzőkkel ruház fel gyűlöletkeltő sértegetések, sztereotípiák vagy elméletek formájában (pl. rosszindulatúak, korruptak, gonoszak stb.), vagy kifejezetten vagy burkoltan azt állítja, hogy a csoport fenyegetést jelent.
- Olyan tartalom vagy beszéd, amely arra próbál ösztönözni másokat, hogy gyűlöljenek vagy diszkrimináljanak embereket azért, mert valamelyik védett csoportba tartoznak.
- Gyűlöletkeltő szimbólumokat (például zászlókat, jelvényeket, felszereléseket) vagy gyűlöletkeltő csoportokra jellemző viselkedési mintákat népszerűsítő tartalmak.

Erőszak

Nem engedélyezünk olyan alkalmazásokat, amelyek indokolatlan erőszakot vagy más veszélyes tevékenységeket mutatnak be vagy segítenek elő. Olyan alkalmazásokat általában engedélyezünk, amelyek játék keretein belül ábrázolnak kitalált erőszakot (ilyenek például a rajzfilmek, a vadászat és a horgászat).

Néhány példa a gyakori irányelvsértésekre:

- Emberekkel vagy állatokkal szemben elkövetett valószerű erőszak vagy erőszakos fenyegetés képi ábrázolása vagy leírása.
- Olyan alkalmazások, amelyek önbántalmazást, öngyilkosságot, étkezési zavarokat, fojtogatást tartalmazó játékokat és egyéb olyan tevékenységeket népszerűsítenek, amelyek súlyos sérülést vagy halált okozhatnak.

Erőszakos szélsőségek

Semmilyen célból (beleértve a toborzást) nem engedélyezzük alkalmazások közzétételét a Google Playen a terroristaszervezeteknek, illetve egyéb veszélyes szervezeteknek vagy olyan mozgalmaknak, amelyek civilek elleni erőszakos cselekedeteket követtek el, készítettek elő vagy vállaltak ilyenért felelősséget.

Nem engedélyezzük az olyan alkalmazásokat, amelyek tartalma erőszakos szélsőségekhez vagy civilek elleni erőszak tervezéséhez, előkészítéséhez vagy ennek dicsőítéséhez kapcsolódik, beleértve azon tartalmakat, amelyek népszerűsítik a terrorcselekményeket, erőszakra buzdítanak, vagy terrortámadásokat ünnepelnek. Ha olyan tartalom kerül közzétételre az erőszakos szélsőségekkel kapcsolatban, amely oktató jellegű, dokumentarista, tudományos vagy művészi összefüggésben értelmezendő, akkor ügyelni kell arra, hogy elegendő információ legyen megadva a releváns EDSA-kontextushoz.

Kényes események

Nem engedélyezünk olyan alkalmazásokat, amelyek valamilyen jelentős társadalmi, kulturális vagy politikai hatással bíró, kényes eseményből (például a lakosságot érintő vészhelyzetből, természeti katasztrófából, közegészségügyi vészhelyzetből, konfliktusból, halálesetből vagy más tragikus eseményből) próbálnak hasznot húzni, vagy nem tapintatosak az ilyen eseménnyel kapcsolatban. A kényes eseményhez kapcsolódó tartalmakat megjelenítő alkalmazásokat általában engedélyezzük, ha az adott tartalom EDSA (Educational, Documentary, Scientific, or Artistic; azaz ismeretterjesztő, oktatási, tudományos és művészeti) jellegű értékekkel bír, vagy ha célja az, hogy felhívja a felhasználók figyelmét a kényes eseményekre.

Néhány példa a gyakori irányelvsértésekre:

- Valós személy vagy csoport öngyilkosság, túladagolás, természetes okok stb. miatti halálával kapcsolatosan tanúsított érzéketlenség.
- Valamely jól dokumentált, jelentős tragédiával járó esemény előfordulásának tagadása.
- Kényes eseményből való haszonszerzés, amely az áldozatok számára nem nyújt semmilyen egyértelmű hasznot.

Bántalmazás és zaklatás

Nem engedélyezzük azokat az alkalmazásokat, melyek fenyegetést, zaklatást vagy bántalmazást tartalmaznak vagy segítenek elő.

Néhány példa a gyakori irányelvsértésekre:

- Nemzetközi vagy vallási konfliktusok áldozatainak bántalmazása.
- Mások kizsákmányolását célzó tartalom, ideértve a kikényszerítést, zsarolást stb.
- Tartalom közzététele valamely személy nyilvános megalázása érdekében.
- Tragikus esemény áldozatai, illetve ismerőseik vagy családtagjaik zaklatása.

Veszélyes termékek

Nem engedélyezzük azokat az alkalmazásokat, melyek elősegítik robbanóanyagok, lőfegyverek, lőszerek vagy bizonyos lőfegyvertartozékok értékesítését.

- A korlátozás alá eső tartozékok közé tartoznak azok az eszközök, amelyek segítségével a lőfegyverek automata tüzelést szimulálhatnak, illetve automata tüzelésre alkalmassá alakíthatók (például a „bump stock”, azaz a rugós válltámasz, a gatling rendszerű elsütőszerkezet, a beilleszthető, automata elsütő billentyű vagy az átalakító készletek). E tartozékok közé tartoznak továbbá a 30-nál több lőszer befogadására alkalmas tárak és hevederek is.

Nem engedélyezzük a robbanóanyagok, lőfegyverek, lőszerek, a korlátozás alá eső lőfegyvertartozékok vagy az egyéb fegyverek gyártására vonatkozó útmutatást biztosító alkalmazásokat. Ide tartozik a lőfegyverek automata, illetve szimulált automata tüzelésre alkalmassá alakításának módjára vonatkozó útmutatás is.

Marihuána

Nem engedélyezzük azokat az alkalmazásokat, melyek elősegítik marihuána vagy marihuánával kapcsolatos termékek értékesítését, függetlenül attól, hogy azok legálisak-e.

Néhány példa a gyakori irányelvsértésekre:

- Lehetőség biztosítása a felhasználóknak arra, hogy alkalmazáson belüli bevásárlókosár funkcióval marihuánát rendeljenek.
- Segítségnyújtás a felhasználóknak marihuána házhoz szállításában vagy átvételében.
- THC-t (tetrahidrokannabinol) tartalmazó termékek (pl. THC-tartalmú CBD-olajok) értékesítésének elősegítése.

Dohány és alkohol

Nem engedélyezzük az olyan alkalmazásokat, amelyek megkönnyítik a dohányáruk vagy nikotintartalmú termékek (például e-cigaretták, vape penek és nikotinos tasakok) értékesítését, vagy az alkohol, dohány vagy nikotin illegális vagy nem megfelelő használatára ösztönöznek.

További információ

- Nem engedélyezett alkohol- vagy dohányfogyasztás és -értékesítés kiskorúak számára történő bemutatása vagy ösztönzése.
- Nem engedélyezett az utalás arra, hogy a dohánytermékek fogyasztása javítja a társadalmi, szexuális, szakmai, szellemi vagy fizikai helyzetet/állapotot.
- Nem engedélyezett a felelőtlen alkoholfogyasztás – így például a túlzott, mértéktelen vagy versenyszerű alkoholfogyasztás – jó fényben való feltüntetése.
- Nem engedélyezettek a dohánytermékkel kapcsolatos hirdetések, promóciók vagy a dohánytermékek kiemelt szerepeltetése (beleértve a hirdetéseket, szalaghirdetéseket, kategóriákat és a dohánytermékeket árusító weboldalakra mutató hivatkozásokat).
- Előfordulhat, hogy korlátozottan engedélyezzük a dohánytermékek értékesítését ételek/áruk házhoz szállítását biztosító alkalmazásokban bizonyos régiókban, életkorszűréssel és biztonsági intézkedésekkel (például: az életkor ellenőrzése kiszállításkor).
- Engedélyezhetjük a nikotinról való leszokást segítő szerként forgalmazott termékek értékesítését az életkorszűrési jogi biztosítékok alapján.

Pénzügyi szolgáltatások

Nem engedélyezzük azokat az alkalmazásokat, melyek megtévesztő vagy kártékony pénzügyi termékeket és szolgáltatásokat kínálnak a felhasználóknak.

A jelen irányelv vonatkozásában pénzügyi termékeknek és szolgáltatásoknak olyan termékeket és szolgáltatásokat tekintünk, melyek pénz és kriptovaluták kezelésével és befektetésével kapcsolatosak, beleértve a személyre szabott tanácsadást nyújtó szolgáltatásokat is.

Ha alkalmazásod pénzügyi termékeket vagy szolgáltatásokat tartalmaz vagy hirdet, akkor az alkalmazás által célzott minden régió és ország állami és helyi jogszabályainak meg kell felelned, például a kötelezően mellékelendő nyilatkozatok tekintetében is.

A pénzügyi funkciókat tartalmazó alkalmazások esetében ki kell tölteni a Play Console-ban található pénzügyi funkciókra vonatkozó nyilatkozati űrlapot.

Bináris opciók

Nem engedélyezzük azokat az alkalmazásokat, melyek bináris opciós kereskedésre nyújtanak lehetőséget a felhasználók számára.

Személyi kölcsönök

A személyi kölcsönt olyan pénzösszegként határozzuk meg, amelyet egy magánszemély, szervezet vagy entitás ad kölcsön egyéni fogyasztónak nem ismétlődő jelleggel, nem tárgyi eszköz megvásárlása vagy oktatás finanszírozása céljából. A személyi kölcsönök fogyasztóinak információra van szükségük a kölcsön minőségéről, jellemzőiről, költségeiről, a visszafizetés ütemérről, a kockázatokról és előnyökről, hogy megalapozott döntéseket hozhassanak a kölcsön felvételéről.

- Például: személyi kölcsönök, fizetésnapi kölcsönök, közösségi kölcsönök, jelzáloghitelek.
- Nem tartoznak ide: ingatlanalapú jelzálogügyletek, autóvásárlási kölcsönök, rulírozó hitelek (például hitelkártyák, folyószámlahitelek).

A személyi kölcsönöket kínáló alkalmazások (nem kizárólagosan beleértve a kölcsönöket közvetlenül kínáló alkalmazások, az ügyfélkeresők, valamint az ügyfeleket harmadik félként szereplő kölcsönzőkkel összekötő alkalmazások) esetében a „Pénzügy” alkalmazáskategóriának kell szerepelnie a Play Console felületén, valamint fel kell tüntetni a következő információkat az alkalmazás metaadataiban:

- a visszafizetés minimális és maximális ideje;
- teljes hiteldíjmutató (THM), amely jellemzően az adott évre vonatkozó kamat, díjak és költségek összege; vagy más hasonló, a helyi jogszabályoknak megfelelően kiszámított ráta;
- a hitel teljes költségét (beleértve a fő és vonatkozó díjakat is) bemutató példa;
- adatvédelmi irányelvek, amelyek részletes tájékoztatást nyújtanak a személyes és bizalmas felhasználói adatokhoz való hozzáférésről, valamint az ilyen adatok begyűjtéséről, felhasználásáról és megosztásáról a jelen irányelvben ismertetett korlátozásoknak megfelelően.

Nem engedélyezünk olyan alkalmazásokat, amelyek a folyósítás napjától számított legfeljebb 60 napon belüli teljes visszafizetést előíró személyi kölcsönt népszerűsítenek (ezt rövid lejáratú személyi kölcsönnek nevezzük).

Az irányelv alól kivételt képezhetnek az olyan országon belül működő személyikölcsön-alkalmazások, ahol konkrét rendeletben meghatározott jogi keretek között kifejezetten engedélyezik a szóban forgó rövid lejáratú kölcsönök gyakorlatát. Ezekben a ritka esetekben a kivételt az adott ország vonatkozó helyi jogszabályaival és szabályozó iránymutatásaival összhangban bíráljuk el.

Meg kell tudnunk állapítani a kapcsolatot a fejlesztői fiók és bármely megadott engedély vagy dokumentáció között, amely azt bizonyítja, hogy személyi kölcsönt folyósíthatsz. További információt vagy dokumentumokat kérhetünk tőled, hogy meggyőződjünk arról, hogy a fiókod megfelel az összes helyi jogszabálynak és rendeletnek.

A személyikölcsön-alkalmazások, az olyan alkalmazások, amelyeknek elsődleges célja a személyi kölcsön felvételének elősegítése (például érdeklődés felkeltése vagy közvetítés), illetve a kiegészítő kölcsönalkalmazások (kölcsönkalkulátor, hitelkalauz stb.) és Earned Wage Access (EWA) alkalmazások nem férhetnek hozzá a bizalmas adatokhoz, úgymint a fotókhoz és a névjegyekhez. A következő engedélyek tiltottak:

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

A bizalmas információt vagy API-ket használó alkalmazásokra további korlátozások és követelmények vonatkoznak. További információért lásd az Engedélyekre vonatkozó szabályzatot.

Magas THM-mel rendelkező személyi kölcsönök

Az Amerikai Egyesült Államokban nem engedélyezzük azokat az alkalmazásokat, melyek 36%-os vagy magasabb THM-mel rendelkező személyi kölcsönöket kínálnak. A személyi kölcsönöket kínáló alkalmazásoknak az Amerikai Egyesült Államokban meg kell jeleníteniük a maximális THM-et, melynek kiszámítását a Truth in Lending Act (TILA) , azaz a kölcsönökre vonatkozó törvény követelményeinek megfelelően kell elvégezni.

Ez az irányelv vonatkozik a kölcsönöket közvetlenül kínáló és az érdeklődést felkeltő alkalmazásokra, valamint az ügyfeleket és harmadik félként szereplő kölcsönzőket összekötő alkalmazásokra is.

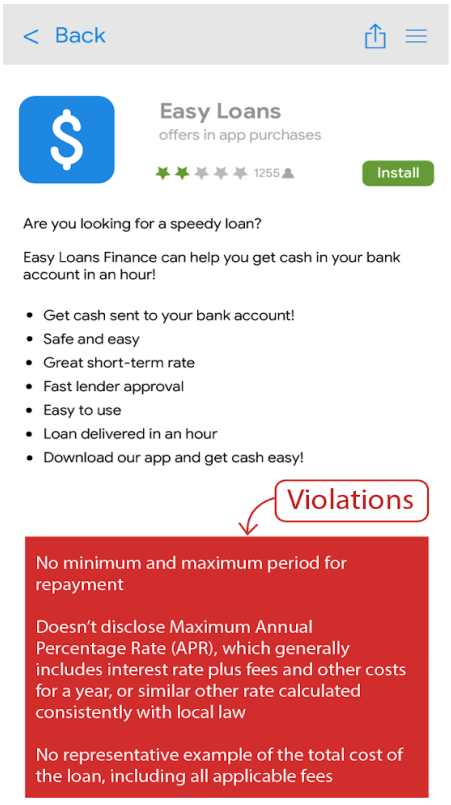
Országspecifikus követelmények

A felsorolt országok felhasználóit célzó, személyi kölcsönt kínáló alkalmazásoknak meg kell felelniük a további követelményeknek, és kiegészítő dokumentációt kell tartalmazniuk a Play Console-ban található pénzügyi funkciókról szóló nyilatkozati űrlap részeként. A Google Play kérésére további információkat vagy dokumentumokat kell benyújtani a vonatkozó szabályozási és engedélyezési követelményeknek való megfelelésről.

1. **India**
   - Ha a Reserve Bank of India (RBI) engedélyével történik a személyi kölcsön biztosítása, akkor be kell nyújtani az engedély másolatát, hogy ellenőrizni tudjuk.
   - Ha az alkalmazás nem közvetlenül nyújt hiteleket, csupán platformot biztosít bejegyzett, nem bankjellegű pénzügyi intézmények (Non-Banking Financial Companies, NBFC) vagy bankok számára a felhasználóknak való hitelnyújtáshoz, akkor ezt a nyilatkozatban pontosan fel kell tüntetni.
     - Továbbá az összes bejegyzett NBFC és bank nevét jól láthatóan fel kell tüntetned az alkalmazásod leírásában.
2. **Indonézia**
   - Ha alkalmazásod információtechnológia-alapú hitelnyújtási szolgáltatást biztosít a 77/POJK.01/2016 számú OJK rendelet (és annak időről időre módosított változata) szerint, be kell küldened érvényes engedélyedet nekünk áttekintésre.
3. **Fülöp-szigetek**
   - Minden, az online kölcsönnyújtó platformokon (Online Lending Platforms, OLP) kölcsönt kínáló pénzügyi és kölcsönt nyújtó vállalat köteles SEC-regisztrációs számmal és hitelesítési tanúsítvánnyal rendelkezni (Certificate of Authority, CA), amelyeket a Fülöp-szigeteki Értékpapír- és Tőzsdebizottságtól (PSEC) kell igényelni.
     - Ezenkívül fel kell tüntetned az alkalmazásod leírásában a vállalatod nevét, üzleti nevedet, PSEC-regisztrációs számodat, illetve az azt igazoló hitelesítési tanúsítványt, hogy pénzügyi vagy kölcsönt kínáló vállalatként tevékenykedhetsz.
   - A kölcsönalapú közösségi finanszírozású tevékenységekben, például peer-to-peer (P2P) kölcsönnyújtásban, illetve a közösségi finanszírozásra irányadó szabályok és előírások (Rules and Regulations Governing Crowdfunding, CF-szabályok) által meghatározott tevékenységekben részt vevő alkalmazásoknak a PSEC-nél bejegyzett CF-közvetítőkön keresztül kell feldolgozniuk a tranzakciókat.
4. **Nigéria**
   - A digitális hitelezőknek (Digital Money Lenders – DML) be kell tartaniuk a nigériai Szövetségi Verseny- és Fogyasztóvédelmi Bizottság (Federal Competition and Consumer Protection Commission – FCCPC) által kiadott és rendszeres időközönként frissülő „LIMITED INTERIM REGULATORY/ REGISTRATION FRAMEWORK AND GUIDELINES FOR DIGITAL LENDING, 2022” (A DIGITÁLIS HITELEZÉSRE VONATKOZÓ KORLÁTOZOTT IDEIGLENES SZABÁLYOZÁSI/REGISZTRÁCIÓS KERETRENDSZER ÉS IRÁNYELVEK, 2022) című dokumentum előírásait, és ellenőrizhető jóváhagyó levéllel kell rendelkezniük az FCCPC-től.
   - A kölcsön szolgáltatójának (loan aggregator) be kell nyújtania a digitális hitelezési szolgáltatásokkal kapcsolatos dokumentumokat és/vagy tanúsítványt, illetve meg kell adnia az elérhetőségi adatokat minden digitális hitelezőpartner esetében.

5. **Kenya**
   - A digitális hitelezőknek (Digital Credit Providers – DCP) végre kell hajtaniuk a DCP regisztrációs folyamatát, és be kell szerezniük a kenyai központi bank (Central Bank of Kenya – CBK) engedélyét. A nyilatkozat részeként be kell nyújtanod a CBK által kiadott engedély másolatát.
   - Ha az alkalmazás nem közvetlenül nyújt hiteleket, csupán platformot biztosít bejegyzett DCP-k számára a felhasználóknak való hitelnyújtáshoz, akkor ezt a nyilatkozatban pontosan fel kell tüntetni, és mellékelni kell a megfelelő partner(ek) DCP-engedélyének másolatát.
   - Jelenleg csak a CBK hivatalos honlapján, a „Directory of Digital Credit Providers" (Digitális hitelszolgáltatók jegyzéke) alatt közzétett szervezetek nyilatkozatait és engedélyeit fogadjuk el.
6. **Pakisztán**
   - Minden nem bankjellegű pénzügyi intézmény (Non-Banking Financial Companies, NBFC) hitelező csak egy digitális hitelező alkalmazást (Digital Lending App, DLA) tehet közzé. Megszüntethetjük azoknak a fejlesztőknek a fejlesztői fiókját és bármely kapcsolódó fiókját, akik egynél több DLA-t kísérelnek meg közzétenni egy-egy NBFC esetében.
   - Igazolnod kell a SECP jóváhagyását arra vonatkozóan, hogy kínálhatsz vagy elősegíthetsz digitális hitelezési szolgáltatásokat Pakisztánban.
7. **Thaiföld**
   - A thaiföldi felhasználókat célzó, 15%-os vagy annál magasabb kamattal járó személyi kölcsönt kínáló alkalmazásoknak érvényes engedéllyel kell rendelkezniük a Bank of Thailandtől (BoT) vagy a Ministry of Finance-tól (MoF). A fejlesztőknek olyan dokumentációt kell benyújtaniuk, amely bizonyítja, hogy képesek személyi kölcsönt nyújtani vagy lebonyolítani Thaiföldön. A dokumentációnak a következőt kell tartalmaznia:
     - A Bank of Thailand által kiadott engedély másolata a személyi kölcsönök szolgáltatójaként vagy nanofinanszírozási szervezetként való működésre vonatkozóan.
     - A Ministry of Finance által kiadott Pico-finance licenc másolata, amely engedélyezi a Pico vagy Pico-plus hitelezőként való működést.

Példa egy gyakori irányelvsértésre:



Szerencsejátékok, játékok és versenyek valódi pénzzel

Engedélyezzük a valódi pénzzel játszott szerencsejáték-alkalmazásokat, a valódi pénzzel játszott szerencsejátékokkal kapcsolatos hirdetéseket, a játékszerűsített kimenetelű hűségprogramokat és a napi sportmenedzserjáték típusú alkalmazásokat, amennyiben megfelelnek bizonyos követelményeknek.

Szerencsejáték-alkalmazások

A Google Play minden egyéb irányelvének betartása mellett lehetőséget biztosítunk arra, hogy az alkalmazások online szerencsejátékot nyújtsanak egyes országokban, amennyiben a fejlesztő végrehajtja a Google Playen terjesztendő szerencsejátékos alkalmazásokhoz szükséges jelentkezési folyamatot , valamint ha az adott országban jóváhagyott állami szerencsejáték-szolgáltatónak minősül és/vagy rendelkezik a vonatkozó állami szerencsejáték-hatóság engedélyével, és bemutatja az adott országban érvényes működési engedélyét a kínált online szerencsejátékos termékre vonatkozóan.

Csak olyan jóváhagyott szerencsejátékos alkalmazásokat engedélyezünk, amelyek a következő típusú online szerencsejátékos termékek valamelyikét nyújtják:

- Online kaszinójátékok
- Sportfogadás
- Lóverseny (amennyiben szabályozása és engedélyezése a sportfogadástól külön történik)
- Lottó
- Napi sportmenedzserjátékok

Az alkalmazásnak a következő feltételeknek kell megfelelnie:

- az alkalmazás Google Playen való terjesztéséhez a fejlesztőnek sikeresen el kell végeznie a jelentkezési folyamatot;
- az alkalmazásnak a terjesztés helyéül szolgáló ország összes vonatkozó jogszabályának és iparági szabványának meg kell felelnie;
- a fejlesztőnek érvényes szerencsejáték-engedéllyel kell rendelkeznie minden olyan országban és államban/területen, ahol az alkalmazást terjeszti;
- a fejlesztő nem nyújthat olyan szerencsejátékos terméket, amelyet szerencsejáték-engedélye nem tesz lehetővé;
- az alkalmazásnak meg kell akadályoznia, hogy kiskorúak használják;
- az alkalmazásnak meg kell akadályoznia, hogy olyan országokban, államokban/területeken vagy földrajzi régiókban használják, ahol a fejlesztő szerencsejáték-engedélye nem érvényes;
- az alkalmazás NEM lehet megvásárolható fizetős alkalmazásként a Google Playen, valamint nem használhatja az Alkalmazáson belüli vásárlás Google Play-számlázása szolgáltatást;
- az alkalmazásnak díjmentesen letölthetőnek és telepíthetőnek kell lennie a Google Play Áruházban;
- az alkalmazásnak AO (kizárólag felnőtteknek, Adult Only), illetve annak megfelelő IARC-besorolással kell rendelkeznie; valamint
- az alkalmazásnak és áruházbeli adatlapjának egyértelműen fel kell tüntetnie a felelősségteljes szerencsejátékkal kapcsolatos információkat.

Egyéb, valódi pénzzel játszott játékok, versenyek és bajnokságok alkalmazásai

A szerencsejáték-alkalmazásokra vonatkozó fenti követelményeknek nem megfelelő, illetve az alábbiakban közzétett „Valódi pénzben játszott egyéb próbajátékok” felsorolásban nem szereplő alkalmazások esetében nem engedélyezünk olyan tartalmakat és szolgáltatásokat, amelyek lehetővé teszik vagy megkönnyítik a felhasználók számára, hogy valódi pénzbeli értékkel rendelkező nyeremény megszerzése érdekében valódi pénzzel (vagy pénzért vásárolt alkalmazáson belüli termékkel) fogadhassanak, licitálhassanak vagy a folyamatban más módon részt vehessenek. Ide tartoznak többek között az online kaszinók, a sportfogadás, a lottójátékok és azok a játékok, amelyek pénzért

pénzbeli vagy más valós értéket képviselő nyereményt kínálnak (kivéve az alább ismertetett, játékszerűsített hűségprogramokra vonatkozó követelmények értelmében engedélyezett programokat).

Példák a használati feltételek megsértésére

- Olyan játékok, amelyek pénzért cserébe lehetőséget nyújtanak fizikai vagy pénzbeli nyeremény megszerzésére.
- Olyan alkalmazások, melyek cselekvésre ösztönző navigációs elemekkel vagy funkciókkal (menüpontok, lapfülek, gombok, WebView-k stb.) buzdítják a valódi pénzzel játszott játékokban, versenyekben vagy bajnokságokban való fogadást, kockáztatást vagy részvételt. Például alkalmazások, melyek „FOGADJ!”, „REGISZTRÁLJ!”, „VERSENYEZZ!” és hasonló szövegekkel invitálják a felhasználókat pénznyeremény lehetőségét nyújtó versenyben való részvételre.
- Alkalmazások, melyek fogadásokat, alkalmazáson belüli fizetőeszközöket, nyereményeket vagy letéteket fogadnak el vagy kezelnek annak érdekében, hogy szerencsejáték útján vagy máshogyan fizikai vagy pénzbeli nyeremény lehetőségét nyújtsák.

Egyéb, valódi pénzzel játszott játékok próbaidőszaka

Időnként korlátozott ideig engedélyezhetjük a valódi pénzben játszott próbajátékok bizonyos típusait a kiválasztott régiókban. A részleteket a Súgó oldalán találod. Az online karomdarus játékok kísérleti programja 2023. július 11-én véget ért Japánban. 2023. július 12-től az online karomdarus játékok a hatályos jogszabályoktól és bizonyos követelmények teljesítésétől függően globálisan megjeleníthetők lesznek a Google Play szolgáltatásban.

Játékszerűsített hűségprogramok

Ha a jogszabályok lehetővé teszik, és szerencsejátékokra vagy más játékokra vonatkozó egyéb követelmények nem érvényesek, a Play Áruház alábbi alkalmassági követelményei mentén engedélyezzük az olyan hűségprogramokat, melyek való életbeli vagy pénzbeli jutalmat nyújtanak a felhasználóknak:

Minden alkalmazás (játékok és nem játékok egyaránt):

- A hűségprogram előnyeinek, jutalmainak egyértelműen másodlagos, kiegészítő szerepet kell játszaniuk az alkalmazásban a megszerzésükhöz szükséges pénzügyi tranzakciókhoz képest (a jutalmakhoz szükséges pénzügyi tranzakcióknak ténylegesen különálló tranzakcióknak kell lenniük, melyek a hűségprogramtól független termék vagy szolgáltatás megvásárlását jelentik), valamint nem képezhetik részét olyan vásárlásnak vagy más tranzakciónak, amely sérti a valódi pénzzel játszott szerencsejátékokra, játékokra és versenyekre vonatkozó irányelv korlátozásait.
  - Például: a szükséges pénzügyi tranzakció egyetlen eleme sem jelenthet olyan nevezési díjat vagy sorsolási nevezést, amely a hűségprogramban való részvétel feltétele, és a szükséges pénzügyi tranzakció nem járhat a megvásárolt termék vagy szolgáltatás átlagos áránál nagyobb költséggel.

Játékalkalmazások :

- A pénzügyi tranzakcióval szerezhető előnyöket vagy jutalmakat biztosító hűségpontok és jutalmak kizárólag fix átváltási aránnyal adhatók és válthatók be, és ezt az arányt egyértelműen feltüntetve dokumentálni kell az alkalmazásban és a program nyilvánosan hozzáférhető hivatalos szabályzatában. A jutalom vagy a beváltható érték megszerzése **nem lehet** tét tárgya, nyeremény, játékosi teljesítményen alapuló eredmény vagy sorsjáték kimenetele.

Nem játékalkalmazások:

- A hűségpontok és a jutalmak akkor lehetnek verseny vagy sorsjáték eredményei, ha megfelelnek a lentebb felsorolt követelményeknek. Az alábbi követelmények vonatkoznak a pénzügyi tranzakcióval szerezhető előnyöket vagy jutalmakat biztosító hűségprogramokra:
  - Az alkalmazásban szerepelnie kell a program hivatalos szabályzatának.

- A változókat tartalmazó, esélyalapú vagy véletlenszerű nyereménnyel járó programok esetében: a program hivatalos feltételei között fel kell tüntetni 1) az esélyeket az olyan nyereménnyel járó programoknál, amelyek rögzített nyerési esélyeket használnak a nyeremény meghatározására; és 2) a kiválasztási módszert (pl. a nyeremény meghatározására szolgáló változókat) minden más ilyen programnál.
- A sorshúzásokat és hasonló promóciókat nyújtó programok hivatalos feltételeinek minden promócióra vonatkozóan meg kell határozniuk, hogy pontosan hány nyertes lehetséges, és mi a nevezés és a sorsolás pontos határideje.
- Az alkalmazásban és a program hivatalos feltételei között egyértelműen dokumentálni kell a hűségpontoknak és a hűségjutalmak halmozódásának rögzített arányát.

Hűségprogramot biztosító alkalmazás típusa	**Hűségprogram játékszerűsítése és változó jutalmak**	**Fix arány/ütem szerinti hűségjutalmak**	**Általános szerződési feltételek a hűségprogramhoz**	**A szerződési feltételeknek közölniük kell a sorsjátékkal járó hűségprogramok esélyeit és kiválasztási módszerét**
Játék	Nem engedélyezzük	Engedélyezzük	Kötelező	Nem vonatkozik (a játékalkalmazások hűségprogramjaiban nem szerepelhetnek sorsjátékszerű elemek)
Nem játék	Engedélyezzük	Engedélyezzük	Kötelező	Kötelező

Alkalmazások a Play Áruházban, melyek szerencsejátékokat és valódi pénzt felhasználó játékokat, versenyeket, bajnokságokat bemutató hirdetéseket jelenítenek meg

A szerencsejátékot, valódi pénzzel játszott játékokat, versenyeket, bajnokságokat hirdető alkalmazásokat engedélyezzük, amennyiben megfelelnek az alábbi követelményeknek:

- az alkalmazásnak és a hirdetésnek (a hirdetőt is beleértve) meg kell felelnie minden olyan terület vonatkozó jogszabályának és iparági szabványának, ahol a hirdetés megjelenik;
- a hirdetésnek az összes népszerűsített szerencsejátékkal kapcsolatos termék és szolgáltatás tekintetében meg kell felelnie a vonatkozó helyi engedélyezési feltételeknek;
- az alkalmazás nem jeleníthet meg szerencsejátékkal kapcsolatos hirdetést 18 éven aluli személyeknek;
- az alkalmazás nem lehet része Az egész családnak programnak;
- az alkalmazás nem célozhat 18 éven aluli személyeket;
- ha az alkalmazás a fenti definíció alapján szerencsejáték-alkalmazást hirdet, a hirdetésnek jól látható tájékoztatást kell nyújtania a felelősségteljes szerencsejátékról a céloldalon, a hirdetett alkalmazás adatlapján, vagy az alkalmazáson belül;
- az alkalmazás nem tartalmazhat szimulált szerencsejátékot (például közösségi kaszinó típusú alkalmazások; virtuális nyerőgépeket tartalmazó alkalmazások);
- az alkalmazás nem tartalmazhat szerencsejátékot vagy valódi pénzzel játszott játékot, lottójátékot, bajnokságot elősegítő funkciót vagy társfunkciót (pl. fogadás vagy kifizetés lehetőségét, sporteredményekről vagy esélyekről szóló adatokat, valamint részvételi díjakat kezelő funkciót);
- az alkalmazás tartalma nem népszerűsíthet szerencsejátékot, valódi pénzzel játszott játékot, lottójátékot vagy bajnokságot, valamint nem irányíthatja a felhasználót ilyen szolgáltatáshoz.

Szerencsejátékokra, valódi pénzzel játszott játékokra, lottójátékokra és bajnokságokra vonatkozó hirdetéseket csak azok az alkalmazások tartalmazhatnak, amelyek megfelelnek a szerencsejáték-

hirdetésekre vonatkozó összes felsorolt követelménynek. Azok az elfogadott (fentebb meghatározott) szerencsejátékos vagy (alább meghatározott) napi sportmenedzser-játékos alkalmazások, amelyek megfelelnek a fenti első hat pontban meghatározott követelményeknek, megjeleníthetnek hirdetéseket szerencsejátékokról, valódi pénzzel játszott játékokról, lottójátékokról és bajnokságokról.

Példák a használati feltételek megsértésére

- Kiskorúaknak készült alkalmazás, amely szerencsejáték-szolgáltatásra vonatkozó hirdetést jelenít meg.
- Szimulált kaszinójáték, amely valódi pénzt használó kaszinót népszerűsít, vagy ilyen kaszinóhoz irányítja a felhasználót.
- Sportesélyek követésével foglalkozó alkalmazás, amely sportfogadási webhelyre vezető szerencsejáték-hirdetéseket tartalmaz.
- Olyan alkalmazás, melynek szerencsejátékkal kapcsolatos hirdetései sértik a megtévesztő hirdetésekre vonatkozó irányelveinket; például olyan hirdetést tartalmaz, amely gombként, ikonként vagy más interaktív alkalmazáson belüli elemként jelenik meg a felhasználó számára.

Napi sportmenedzserjáték (DFS) kategóriájú alkalmazások

Csak akkor engedélyezzük a napi sportmenedzserjáték (daily fantasy sports, DFS) kategóriájú alkalmazásokat (a helyi jogszabályok szerinti meghatározásoknak megfelelően), ha megfelelnek az alábbi követelményeknek:

- az alkalmazás vagy 1) csak az Amerikai Egyesült Államokban kerül terjesztésre, vagy 2) az Amerikai Egyesült Államoktól eltérő országok esetében a fentebb látható, szerencsejáték-alkalmazásokra vonatkozó követelmények és jelentkezési folyamat alapján engedélyezhető;
- az alkalmazás Playen való terjesztése előtt a fejlesztőnek sikeresen végre kell hajtania a DFS-alkalmazásokra vonatkozó jelentkezést , és szükség van az alkalmazás jóváhagyására;
- az alkalmazásnak a terjesztés helyéül szolgáló országok minden vonatkozó jogszabályának és iparági szabványának meg kell felelnie;
- az alkalmazásnak meg kell akadályoznia, hogy kiskorú felhasználók fogadásokat kössenek és pénzügyi tranzakciókat végezzenek az alkalmazásban;
- az alkalmazás NEM lehet megvásárolható fizetős alkalmazásként a Google Playen, valamint nem használhatja az Alkalmazáson belüli vásárlás Google Play-számlázása szolgáltatást;
- az alkalmazásnak ingyenesen letölthetőnek és telepíthetőnek kell lennie az Áruházban;
- az alkalmazásnak AO (kizárólag felnőtteknek, Adult Only), illetve annak megfelelő IARC-besorolással kell rendelkeznie;
- az alkalmazásnak és áruházbeli adatlapjának egyértelműen fel kell tüntetnie a felelősségteljes szerencsejátékkal kapcsolatos információkat;
- az alkalmazásnak a terjesztés helyéül szolgáló USA-állam és -terület összes vonatkozó jogszabályának és iparági szabványának meg kell felelnie;
- a fejlesztőnek érvényes engedéllyel kell rendelkeznie az összes olyan USA-államban és -területen, ahol engedélykötelesek a napi sportmenedzserjáték kategóriájú alkalmazások;
- az alkalmazásnak meg kell akadályoznia a használatát az összes olyan USA-államban és -területen, amelyekhez a fejlesztő nem rendelkezik a napi sportmenedzserjáték kategóriájú alkalmazásokhoz szükséges engedéllyel; és
- az alkalmazásnak meg kell akadályoznia a használatát az összes olyan USA-államban és -területen, amelyben nem legálisak a napi sportmenedzserjáték kategóriájú alkalmazások.

Jogsértő tevékenységek

Nem engedélyezzük azokat az alkalmazásokat, amelyek jogsértő tevékenységeket reklámoznak vagy segítenek elő.

Néhány példa a gyakori irányelvsértésekre:

- Illegális kábítószerek eladásának vagy megvásárlásának elősegítése.
- Kiskorúak kábítószer-, alkohol- vagy dohányfogyasztásának bemutatása vagy ösztönzése.
- Illegális kábítószerek termesztésére vagy készítésére vonatkozó útmutató.

Felhasználó által létrehozott tartalom

A felhasználó által létrehozott tartalom olyan tartalom, amelyet a felhasználók biztosítanak az alkalmazásnak, és amely az alkalmazás felhasználóinak legalább egy része által látható és hozzáférhető.

A felhasználói tartalmat tartalmazó vagy megjelenítő alkalmazások, beleértve azokat az alkalmazásokat is, amelyek olyan specializált böngészők vagy kliensek, amelyek felhasználói tartalom platformjára irányítják a felhasználókat, kötelesek olyan stabil, hatékony és folyamatos felhasználóitartalom-moderálást fenntartaniuk, amelyre igazak az alábbiak:

- Megköveteli a felhasználótól az alkalmazáshoz tartozó általános szerződési feltételek és/vagy felhasználói szabályzat elfogadását, mielőtt a felhasználó tartalmat hozhat létre vagy tölthet fel.
- Meghatározza a kifogásolható tartalmakat és viselkedéseket (a Google Play Fejlesztői Programszabályzatnak megfelelő módon), és tiltja őket az alkalmazás általános szerződési feltételeiben vagy felhasználói szabályzatában.
- A felhasználói tartalom moderálását az alkalmazás által nyújtott felhasználói tartalmak típusának megfelelően, észszerűen elvárható mértékben valósítja meg. Ennek részeként alkalmazáson belüli rendszert biztosít a kifogásolható felhasználói tartalom és felhasználók bejelentésére és letiltására, valamint szükség esetén lépéseket tesz a felhasználói tartalommal vagy a felhasználókkal szemben. A különféle felhasználói tartalomélmények különböző moderálást igényelhetnek. Például:
  - Az olyan felhasználói tartalmat megjelenítő alkalmazásoknak, amely a felhasználók meghatározott körét felhasználó-ellenőrzéssel, offline regisztrációval vagy hasonló módszerekkel azonosítja (például kizárólag egy konkrét iskola, vállalat stb. által használt alkalmazásoknak), a tartalom vagy felhasználók bejelentésére szolgáló, alkalmazáson belüli funkcióval kell rendelkezniük.
  - A meghatározott felhasználókkal 1:1 (kétszemélyes) felhasználói interakciót (például közvetlen üzenetváltást, megjelelölést, megemlítést stb.) lehetővé tévő felhasználói tartalmon alapuló funkcióknak alkalmazáson belüli funkciót kell biztosítania a felhasználók letiltására.
  - A nyilvánosan elérhető felhasználói tartalomhoz hozzáférést nyújtó alkalmazásoknak – mint például a közösségi hálózati és a bloggeralkalmazásoknak – a felhasználók és tartalom bejelentésére, valamint a felhasználók letiltására szolgáló, alkalmazáson belüli funkciót kell biztosítaniuk.
  - Kiterjesztett valóságot (AR) használó alkalmazások esetén a felhasználói tartalmak moderálásának (beleértve az alkalmazáson belüli bejelentési rendszert is) felelnie kell a kifogásolható felhasználói AR-tartalmakért (például nyíltan szexuális jellegű AR-képek), valamint az érzékeny AR-helyszínekért is (például tiltott területek: katonai bázis vagy magánterület, ahol az AR-tartalmak problémát okozhatnak a tulajdonos számára).
- Óvintézkedésekkel akadályozza meg, hogy az alkalmazáson belüli bevételszerzési lehetőség kifogásolható felhasználói viselkedésre buzdítson.

Alkalomszerű szexuális tartalmak

A szexuális tartalom „alkalomszerűnek” tekintendő, ha olyan felhasználóitartalom-alkalmazásban jelenik meg, amely (1) elsősorban nem szexuális jellegű tartalomhoz kínál hozzáférést, illetve (2) nem aktívan népszerűsít vagy javasol szexuális jellegű tartalmat. A vonatkozó jogszabályok értelmében illegálisnak minősülő szexuális tartalmat és a gyermekeket veszélyeztető tartalmat nem tekintjük „alkalomszerűnek”, és nem engedélyezzük.

A felhasználóitartalom-alkalmazások tartalmazhatnak „alkalomszerű” szexuális tartalmat, ha teljesülnek a következő feltételek:

- Alapértelmezés szerint az ilyen tartalmat olyan szűrő rejti el, amelynek kikapcsolásához legalább két felhasználói művelet szükséges (pl. közbeiktatással elérhetetlenné tétel vagy elrejtés szem elől alapértelmezés szerint, kivéve, ha a „biztonságos keresés” ki van kapcsolva).
- A családokkal kapcsolatos irányelv értelmében életkorszűrő rendszerek, úgymint semleges életkorszűrés vagy a vonatkozó jogszabályok által meghatározott, megfelelő rendszer használata kifejezetten gátolja, hogy gyermekek férjenek hozzá az alkalmazáshoz.
- Az alkalmazásod megfelelő válaszokat ad a felhasználói tartalom besorolásával kapcsolatos kérdőívre, a tartalombesorolási irányelv által meghatározott módon.

Az olyan alkalmazásokat, amelyek elsődleges célja felhasználó által létrehozott kifogásolható tartalmak terjesztése, eltávolítjuk a Google Play rendszeréből. Ehhez hasonlóan szintén eltávolítjuk a Google Play rendszeréből azokat az alkalmazásokat, melyeket elsődlegesen felhasználók által létrehozott kifogásolható tartalmak terjesztésére használnak, valamint azokat, amelyek a felhasználók között olyan hírnévre tesznek szert, hogy jó helynek számítanak az ilyen tartalmak terjesztésére.

Néhány példa a gyakori irányelvsértésekre:

- Felhasználó által létrehozott, a szexualitást nyíltan megjelenítő tartalom reklámozása, beleértve olyan fizetős funkciók megvalósítását vagy engedélyezését, amelyek lényege a kifogásolható tartalmak megosztásának ösztönzése.
- Alkalmazások felhasználók által létrehozott olyan tartalmakkal, amelyekben nincs megfelelő óvintézkedés a fenyegetéssel, zaklatással vagy bántalmazással szemben, különösképpen ha az kiskorúak ellen irányul.
- Olyan bejegyzések, megjegyzések vagy fotók egy alkalmazáson belül, amelyek elsődleges célja a másik személy zaklatása vagy kiszemelése visszaélések elkövetése, rosszindulatú támadás vagy kigúnyolás céljából.
- Olyan alkalmazások, amelyek folyamatosan figyelmen kívül hagyják a kifogásolható tartalmakkal kapcsolatos felhasználói panaszokat.

Egészségügyi tartalom és szolgáltatás

Nem engedélyezünk olyan alkalmazásokat, amelyek kártékony egészségügyi tartalmat és szolgáltatást kínálnak a felhasználóknak.

Ha az alkalmazása egészségügyi tartalmat vagy szolgáltatásokat hirdet, gondoskodnia kell arról, hogy alkalmazása megfeleljen valamennyi vonatkozó jogszabálynak és rendeletnek.

Egészséggel kapcsolatos alkalmazások

Ha alkalmazásod egészségügyi adatokhoz fér hozzá, és egészségügyi alkalmazás, vagy egészséggel kapcsolatos funkciókat kínál, meg kell felelnie a Google Play meglévő fejlesztői irányelveinek (beleértve az Adatvédelemre, megtévesztésre és visszaélésekre, valamint a Kényes eseményekre vonatkozókat), illetve az alábbi követelményeknek:

- **Play Console-nyilatkozat:**
  - Lépj a Play Console Alkalmazástartalom oldalára (Irányelvek > Alkalmazástartalom), majd válaszd ki azt a kategóriát (vagy kategóriákat), amelybe az alkalmazásod tartozik.
- **Adatvédelmi irányelvekre és jól látható nyilatkozatra vonatkozó követelmények:**
  - Az alkalmazáshoz közzé kell tenni az adatvédelmi irányelvekre mutató linket a Play Console megfelelő mezőjében, továbbá az adatvédelmi irányelvekre mutató linket vagy az adatvédelmi irányelvek szövegét magában az alkalmazásban. Gondoskodni kell arról, hogy az adatvédelmi irányelvek aktív, nyilvánosan hozzáférhető és geokerítéssel nem védett URL-címen álljanak rendelkezésre (PDF nem megengedett), és hogy ne legyenek szerkeszthetők (az Adatbiztonság szakasznak megfelelően).

- Az alkalmazás adatvédelmi irányelveinek az alkalmazáson belüli esetleges adatvédelmi nyilatkozatokkal együtt átfogóan ismertetniük kell a személyes vagy bizalmas felhasználói adatokhoz való hozzáférést, illetve az ilyen adatok gyűjtését, felhasználását és megosztását, a fenti Adatbiztonság szakaszban közzétett adatokon túl. A veszélyes vagy futtatáskor kért engedélyek által szabályozott funkciók vagy adatok esetében az alkalmazásnak meg kell felelnie a jól látható közlésre és a hozzájárulásra vonatkozó követelményeknek.
- Nem kérhető olyan engedély, amely nem szükséges az egészségügyi alkalmazás alapvető funkcióinak ellátásához, a nem használt engedélyeket pedig el kell távolítani. Az egészséghez fűződő bizalmas adatok körében fontolóra vett engedélyek listáját itt találod: Egészségügyi alkalmazások kategóriái és további információk.
- Ha az alkalmazás elsősorban nem egészségügyi alkalmazás, ám vannak egészségügyi funkciói, és egészségügyi adatokhoz fér hozzá, akkor még az egészségügyi alkalmazásokra vonatkozó irányelv hatálya alá tartozik. Legyen egyértelmű a felhasználó számára, hogy milyen kapcsolat van az alkalmazás alapvető funkciója és az egészségügyi adatok gyűjtése között (például biztosítók, olyan játékalkalmazások, amelyek a játékbeli előrehaladás érdekében gyűjtik a felhasználó tevékenységadatait, stb.). Ezt a korlátozott felhasználási módot az alkalmazás adatvédelmi irányelveinek tükrözniük kell.

- **További követelmények:**
  Ha egészségügyi alkalmazásod a következő besorolások valamelyikére jogosult, a releváns követelményeknek is meg kell felelned azon kívül, hogy kiválasztod a megfelelő kategóriát a Play Console-ban:
  - **Kormányzattal kapcsolatban álló egészségügyi alkalmazások:** Ha az állam vagy egy elismert egészségügyi szervezet engedélyt adott neked arra, hogy velük együttműködve kifejlessz és terjessz egy alkalmazást, be kell küldened a jogosultságod igazolását az előzetes értesítési űrlapon.
  - **Kontaktuskövető/egészségügyi állapotot jelző alkalmazás:** Ha az alkalmazásod kontaktuskövető, illetve egészségügyi állapotot jelző alkalmazás, akkor a Play Console-ban válaszd a Disease Prevention and Public Health (Járványmegelőzés és közegészségügy) lehetőséget, és add meg a szükséges információkat a fenti előzetes értesítési űrlapon.
  - **Emberi alanyokon végzett kutatásokkal kapcsolatos alkalmazások:** Az egészséggel kapcsolatos, emberi alanyokon végzett kutatásokat támogató alkalmazásoknak be kell tartaniuk minden szabályt és előírást, beleértve, de nem kizárólagosan, a résztvevők, illetve kiskorúak esetében a szülő vagy gyám beleegyező nyilatkozatának beszerzését. Az egészségügyi kutatást végző alkalmazásoknak felmentés hiányában az Intézményi Felülvizsgálati Bizottság (IFB), illetve azzal egyenértékű, független etikai bizottság jóváhagyását is meg kell szerezniük. Kérésre igazolni kell a jóváhagyás meglétét.
  - **Orvosieszköz- vagy SaMD-alkalmazások:** Az orvosi eszköznek vagy orvosi eszközként működő szoftvernek (SaMD) minősülő alkalmazásoknak olyan engedélyezési igazolást vagy más jóváhagyó dokumentumot kell beszerezniük és megőrizniük, amelyet az egészségügyi alkalmazás irányításáért és megfelelőségéért felelős szabályozó hatóság vagy testület adott ki. Kérésre igazolni kell az engedély vagy jóváhagyás meglétét.

Health Connect-adatok

A Health Connect-engedélyek révén elért adatok a felhasználói adatokra vonatkozó irányelv szerinti személyes és érzékeny felhasználói adatnak minősülnek, valamint a következő további követelmények vonatkoznak rájuk:

Vényköteles gyógyszerek

Nem engedélyezünk olyan alkalmazásokat, amelyek elősegítik a vényköteles gyógyszerek vény nélküli értékesítését vagy megvásárlását.

Nem engedélyezett szerek

A jogszerűségre vonatkozó állításoktól függetlenül a Google Play nem engedélyezi a jóvá nem hagyott szereket népszerűsítő, illetve értékesítő alkalmazásokat.

Néhány példa a gyakori irányelvsértésekre:

- Minden olyan tétel, amely szerepel ezen a tiltott gyógyszerekről és táplálékkiegészítőkről készült, nem teljes listán.
- Efedrát tartalmazó termékek.
- Humán koriongonadotropint (hCG) tartalmazó termékek, amennyiben népszerűsítésük testsúlycsökkenéssel kapcsolatosan vagy anabolikus szteroidok népszerűsítése mellett történik.
- Veszélyes alkotóelemeket vagy aktív összetevőként gyógyszereket tartalmazó gyógynövénykészítmények és táplálékkiegészítők.
- Az egészséggel kapcsolatos hamis vagy félrevezető állítások, többek között annak állítása, hogy az adott termék ugyanolyan hatékony, mint a vényköteles gyógyszerek vagy az ellenőrzött anyagok.
- Olyan, a kormányzati szervek által jóvá nem hagyott termékek, amelyek reklámja azt sugallja, hogy a termék biztonságos, illetve hatékony valamely betegség megelőzésében, gyógyításában vagy kezelésében.
- Olyan termékek, amelyekkel kapcsolatban valamilyen kormányzati vagy hatósági intézkedést foganatosítottak, illetve figyelmeztetést adtak ki.
- Olyan névvel rendelkező termékek, amelyek megtévesztően hasonlítanak valamely nem engedélyezett gyógyszer, táplálékkiegészítő vagy szabályozott anyag nevére.

Ha többet szeretnél tudni arról, hogy mely nem jóváhagyott vagy megtévesztő gyógyszereket és táplálékkiegészítőket kísérjük figyelemmel, keresd fel a www.legitscript.com webhelyet.

Az egészséggel kapcsolatos téves információ

Nem engedélyezünk az egészséggel kapcsolatos félrevezető, a fennálló orvostudományi közmegegyezéssel ellentétes, vagy olyan állítást tartalmazó alkalmazást, amely kárt okozhat a felhasználóknak.

Néhány példa a gyakori irányelvsértésekre:

- Oltóanyaggal kapcsolatos félrevezető állítások, például hogy az oltóanyag megváltoztathatja a DNS-t.
- Káros, jóváhagyással nem rendelkező kezelések támogatása
- Más kártékony egészségügyi gyakorlatok, így például a konverziós terápia támogatása.

Egészségügyi funkciók

Nem engedélyezzük a gyógyászati vagy egészségügyi témájú funkciókat kínáló olyan alkalmazásokat, amelyek megtévesztőek vagy potenciálisan károsak. Például nem engedélyezünk olyan alkalmazásokat, amelyek kizárólag alkalmazásalapú oximéter funkciót kínálnak. Az oximéter alkalmazásokhoz külső hardver, hordható eszköz vagy kifejezetten az oximéter funkció támogatásához készült okostelefonos érzékelők is szükségesek. E támogatott alkalmazásoknak jogi nyilatkozatot kell feltüntetniük a metaadatokban, amely kimondja, hogy az alkalmazás nem orvosi használatra készült, kizárólag általános fittségi és jólléti célokat szolgál, nem orvosi eszköz, illetve megfelelően fel kell tüntetni a kompatibilis hardver- vagy eszközmodelleket.

Kifizetések – klinikai szolgáltatások

A szabályozott egészségügyi szolgáltatásokat érintő tranzakciók nem használhatják a Google Play számlázási rendszerét. További információ A Google Play fizetési irányelveinek ismertetése című súgócikkben található.

Blokkláncalapú tartalom

A blokklánc-technológia folyamatosan és gyorsan fejlődik, ezért az a célunk, hogy olyan platformot biztosítsunk a fejlesztőknek, amelyen új dolgokat alkothatnak, és gazdagabb, átélhetőbb élményekben részesíthetik a felhasználókat.

A jelen irányelv vonatkozásában a blokkláncalapú tartalmakat blokkláncon tárolt tokenizált digitális eszközöknek tekintjük. Ha alkalmazásod blokkláncalapú tartalommal rendelkezik, meg kell felelned ezeknek a követelményeknek.

Kriptotőzsdék és szoftveres tárcák

Csak a szabályozott joghatóságokban, tanúsított szolgáltatásokon keresztül lehet kriptovalutákat vásárolni, tartani őket vagy kereskedni velük.

Az alkalmazásod által célzott régió vagy ország vonatkozó jogszabályainak is meg kell felelned, illetve nem teheted közzé alkalmazásodat azokon a helyeken, ahol a termékeid vagy szolgáltatásaid be vannak tiltva. A Google Play további információt vagy dokumentumokat kérhet tőled annak igazolására, hogy megfelelsz a vonatkozó szabályozói vagy licencelési követelményeknek.

Kriptovaluták bányászata

Nem engedélyezzük azokat az alkalmazásokat, melyek kriptovalutát bányásznak az eszközökön. Engedélyezzük azokat az alkalmazásokat, amelyek távolról irányítják a kriptovaluta bányászatát.

Tokenizált digitális eszközök terjesztéséhez kapcsolódó átláthatósági követelmények

Ha alkalmazásod tokenizált digitális eszközöket értékesít, vagy lehetővé teszi a felhasználóknak ezek megszerzését jutalomként, be kell ezt jelentened a Play Console Alkalmazástartalom oldalán szereplő Pénzügyi funkciók nyilatkozati űrlapon.

Alkalmazáson belüli termék létrehozásakor jelölnöd kell a részletes termékadatoknál, hogy az adott termék tokenizált digitális eszköz. További útmutatás: Alkalmazáson belüli termék létrehozása.

Nem promotálhatod vagy népszerűsítheted a játékból vagy kereskedelmi tevékenységből származó potenciális nyereségeket.

Az NFT-gamifikációval kapcsolatos további körülmények

A Google Play Valódi pénzzel játszott szerencsejátékokra, játékokra és versenyekre vonatkozó irányelvének megfelelően azoknak a szerencsejáték-alkalmazásoknak is teljesíteniük kell a jelentkezési eljárást, amelyek tokenizált digitális eszközöket (például NFT-ket) integrálnak.

A szerencsejáték-alkalmazásokra vonatkozó követelményeknek nem megfelelő és az Egyéb, valódi pénzzel játszott játékok próbaidőszaka részben nem szereplő alkalmazások esetében semmilyen pénzbeli értéket képviselő dolog nem fogadható el ismeretlen értékű NFT megszerzésének esélyéért cserébe. A felhasználók által vásárolt NFT-ket a játékban kell feldolgozni vagy felhasználni a felhasználói élmény javítása vagy a játékbeli előrehaladás segítésének céljából. Az NFT-k nem használhatók arra, hogy a felhasználó valódi pénzbeli értékkel rendelkező nyeremény (beleértve az egyéb NFT-ket) megszerzésének esélyére fogadjon vagy licitáljon.

Néhány példa a gyakori irányelvsértésekre:

- Olyan alkalmazások, amelyek NFT-csomagokat árusítanak úgy, hogy nem közlik a csomag pontos tartalmát és a benne található NFT-k értékét.
- Olyan befizetést igénylő közösségi kaszinójátékok (például nyerőgépek), amelyekkel NFT-ket lehet nyerni.

AI által létrehozott tartalom

Ahogy a generatív AI-modellek a fejlesztők szélesebb körének állnak rendelkezésére, lehet, hogy az elköteleződés erősítése és a felhasználói élmény javítása érdekében te is beépíted ezeket a modelleket az alkalmazásaidba. A Google Play segíteni szeretne abban, hogy az AI által létrehozott tartalom minden felhasználó számára biztonságos legyen, és a felhasználói visszajelzések felhasználása biztosítsa a felelős innovációt.

AI által létrehozott tartalom

Az AI által létrehozott tartalom olyan tartalom, amelyet felhasználói utasítás alapján generatív AI-modell alkotott. AI által létrehozott tartalom például többek között:

- a szöveges formában beszélgetést folytató, generatív AI-csevegőrobotok, amelyekben a csevegőrobottal való interakció az alkalmazás központi jellemzője;
- szöveges, képi, vagy hangutasítás alapján az AI által generált kép.

A felhasználói biztonság érdekében és a Google Play irányelveinek hatályával összhangban az AI használatával tartalmat létrehozó alkalmazásoknak be kell tartaniuk a meglévő Google Play fejlesztői irányelveket, beleértve a korlátozott tartalom (úgymint a gyermekek kizsákmányolását vagy a gyermekekkel való visszaélést elősegítő tartalom és a megtévesztő viselkedést lehetővé tévő tartalom) létrehozásának tiltását és megelőzését.

Az AI használatával tartalmat létrehozó alkalmazásoknak alkalmazáson belüli felhasználói bejelentési vagy -megjelölési funkciót kell tartalmazniuk, amely lehetővé teszi, hogy a felhasználók anélkül jelenthessék be vagy jelölhessék meg a sértő tartalmakat a fejlesztőknek, hogy ki kellene lépniük az alkalmazásból, A fejlesztők pedig a felhasználói bejelentéseket felhasználva finomítják a tartalomszűrést és -moderálást az alkalmazásaikban.

Szellemi tulajdon

Nem engedélyezzük a mások szellemi tulajdonjogait (például védjegyeket, szerzői jogokat, szabadalmakat, kereskedelmi titkokat és egyéb tulajdonjogokat) sértő alkalmazásokat és fejlesztői fiókokat. Azokat az alkalmazásokat sem engedélyezzük, amelyek bátorítják vagy támogatják a szellemi tulajdonjogok megsértését.

Minden, a szerzői jog vélelmezett megsértésével kapcsolatos bejelentést kivizsgálunk. Ha további információra van szüksége, illetve ha DMCA-kérelmet szeretne benyújtani, tekintse át a szerzői joggal kapcsolatos eljárásaink dokumentációját.

Ha panaszt szeretne benyújtani valamelyik alkalmazáson belüli értékesítéssel vagy promócióval szemben hamisított árucikkek értékesítése miatt, küldjön be egy hamisítási értesítést .

Ha Ön védjegytulajdonos, és úgy véli, hogy a Google Playen megtalálható valamelyik alkalmazás sérti a védjegyhez fűződő jogait, a probléma rendezésével kapcsolatban forduljon közvetlenül a fejlesztőhöz. Ha nem sikerül megállapodnia a fejlesztővel, nyújtson be védjeggyel kapcsolatos panaszt ezen az űrlapon .

Ha írásos dokumentummal tudja bizonyítani, hogy joga van a harmadik fél szellemi tulajdonának (pl. márkanevének, logójának vagy grafikai elemeinek) használatára az alkalmazásában vagy áruházi adatlapján, vegye fel a kapcsolatot a Google Play csapatával , mielőtt beküldené a jelentkezését, így ugyanis gondoskodni tud arról, hogy az alkalmazását ne utasítsák el a szellemi tulajdonjogok megsértése miatt.

Szerzői joggal védett tartalom illetéktelen használata

Nem engedélyezzük azokat az alkalmazásokat, amelyek sértik a szerzői jogot. A szerzői joggal védett tartalom módosítása is sértheti irányelveinket. A fejlesztőket kötelezhetjük arra, hogy szolgáltassanak bizonyítékot a védett tartalom használati jogára vonatkozóan.

Nagyon figyeljen oda, amikor szerzői jog által védett tartalmat használ az alkalmazás működésének bemutatására. Általánosságban elmondható, hogy az eredeti tartalom készítése a legbiztonságosabb.

Néhány példa a gyakori irányelvsértésekre:

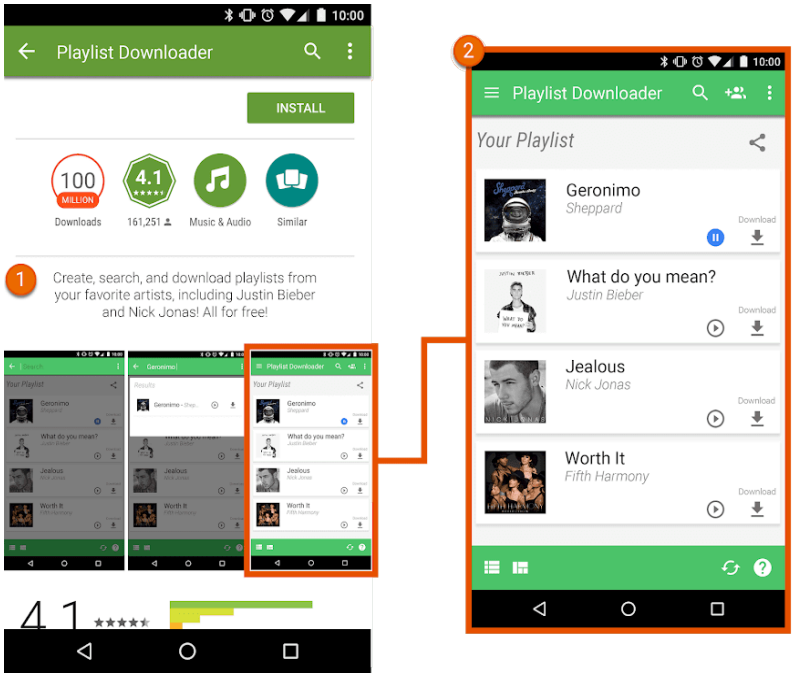
- Borítókép zenei albumokhoz, videójátékokhoz és könyvekhez.
- Marketingképek filmekből, tévéműsorokból vagy videójátékokból.
- Rajzok és egyéb képek képregényekből, rajzfilmekből, filmekből, videóklipekből vagy tévéműsorokból.
- Egyetemi és profi sportcsapatok emblémái.
- Közszereplő közösségimédia-fiókjaiból vett fotók.
- Profi fotósok közszereplőkről készített képei.
- A szerzői joggal védett eredeti műtől nem megkülönböztethető reprodukciók vagy „rajongói alkotások”.
- Szerzői joggal védett hanganyagból részleteket lejátszó alkalmazások.
- Olyan könyvek reprodukciója vagy fordítása, amelyek nem számítanak közkincsnek.

Buzdítás a szerzői jogok megsértésére

Nem engedélyezzük azokat az alkalmazásokat, amelyek támogatják vagy bátorítják a szerzői jogok megsértését. Mielőtt közzétenné alkalmazását, gondolja végig, hogy alkalmazása ösztönöz-e a szerzői jogok megsértésére, szükség esetén pedig kérjen jogi tanácsot.

Néhány példa a gyakori irányelvsértésekre:

- Streamelésre alkalmas alkalmazások, amelyek lehetővé teszik a felhasználók számára szerzői joggal védett tartalmak engedély nélküli letöltését helyi példányként.
- Alkalmazások, amelyek szerzői joggal védett alkotások (zenei és videótartalmak) streamelésére és letöltésére ösztönzik a felhasználókat, így sértik a vonatkozó szerzői jogi jogszabályokat:



① Az alkalmazás leírása arra bátorítja a felhasználókat, hogy engedély nélkül töltsenek le szerzői jog által védett tartalmakat.
② Az alkalmazás adatlapján lévő képernyőkép arra bátorítja a felhasználókat, hogy engedély nélkül töltsenek le szerzői jog által védett tartalmakat.

Védjegyhez kapcsolódó jogsértés

Nem engedélyezzük azokat az alkalmazásokat, amelyek sértik mások védjegyhez fűződő jogait. A védjegy egy olyan szó, szimbólum vagy ezek kombinációja, amely a termék vagy szolgáltatás forrását azonosítja. A védjegy megszerzése után a tulajdonos kizárólagos jogokat kap a védjegy használatára az adott termékekkel vagy szolgáltatásokkal kapcsolatban.

A védjegyjogok megsértése az ugyanolyan vagy hasonló védjegy nem megfelelő vagy jogosulatlan, olyan módon történő használata, amely nagy valószínűséggel zavart okoz a szóban forgó termék forrásának megállapításában. Ha alkalmazása oly módon használja fel valamely másik fél védjegyeit, hogy az valószínűleg zavart okoz, akkor az alkalmazást felfüggeszthetjük.

Hamisítás

Nem engedélyezzük azokat az alkalmazásokat, amelyek hamisított árucikkeket értékesítenek, illetve ezt a tevékenységet népszerűsítik. A hamisított árucikkek egy másik termék védjegyével azonos, illetve attól alig megkülönböztethető védjegyet vagy emblémát tartalmaznak. A termék márkajegyeit lemásolva azt a látszatot próbálják kelteni a vásárlókban, hogy a hamisított árucikk a márkatulajdonos eredeti terméke.

Adatvédelem, megtévesztés és visszaélésszerű eszközhasználat

Elkötelezettek vagyunk a felhasználói adatok védelme, valamint a biztonságos felhasználói környezet megteremtése iránt. Szigorúan tiltjuk a hálózatokkal, eszközökkel vagy személyes adatokkal visszaélő, a megtévesztő és a rosszindulatú alkalmazásokat.

Felhasználói adatok

A fejlesztőnek a felhasználói adatokat (például a felhasználóktól vagy a felhasználókról gyűjtött adatokat, beleértve az eszközadatokat is) átlátható módon kell kezelnie. Ez azt jelenti, hogy nyilvánosságra kell hozni a felhasználói adatok hozzáférését, gyűjtését, felhasználását, kezelését és megosztását az alkalmazásból, és az adatok felhasználását a nyilvánosságra hozott irányelveknek megfelelő célokra kell korlátozni. Kérjük, vedd figyelembe, hogy a személyes és érzékeny felhasználói adatok bárminemű kezelésére érvényes még minden, az alábbi „Személyes és bizalmas felhasználói adatok” című szakaszban feltüntetett további követelmény is. Ezek a Google Play-követelmények kiegészítik a vonatkozó adatvédelmi jogszabályok által előírt valamennyi követelményt.

Ha harmadik féltől származó kódot (például SDK-t) szerepeltetsz az alkalmazásodban, akkor biztosítanod kell, hogy az alkalmazásodban használt, harmadik fél által biztosított kód, valamint az alkalmazásodból származó adatok harmadik fél általi feldolgozására irányuló gyakorlatok megfeleljenek a Google Play Fejlesztői Programszabályzatnak, amely a felhasználásra és a közzétételre vonatkozó előírásokat is tartalmaz. Biztosítanod kell például, hogy az SDK-szolgáltatók ne adjanak el személyes és érzékeny felhasználói adatokat az alkalmazásból. Ez a követelmény attól függetlenül érvényes, hogy a felhasználói adatok továbbítása a szerverre történő elküldés után vagy harmadik fél kódjának az alkalmazásba történő beágyazásával történik.

Személyes és bizalmas felhasználói adatok

A személyes vagy bizalmas felhasználói adatok közé tartoznak többek között a személyazonosításra alkalmas adatok, a pénzügyi, fizetési és hitelesítési adatok, a telefonkönyvvel, a névjegyekkel, az eszköz helyével , az SMS-ekkel és a hívásokkal kapcsolatos adatok, az egészségügyi adatok , a Health Connect-adatok , az eszközön található egyéb alkalmazások készlete, a mikrofon és a kamera adatai, továbbá egyéb bizalmas eszköz- vagy használati adatok. Ha az alkalmazás személyes és bizalmas felhasználói adatokat kezel, akkor a következőkre kell ügyelni:

- Az alkalmazásban megszerzett személyes és bizalmas felhasználói adatokhoz való hozzáférést, valamint ezek gyűjtését, felhasználását és megosztását az alkalmazásra és a szolgáltatás funkcióira

és az irányelvekben feltüntetett célokra kell korlátozni a felhasználó által észszerűen elvárható módon:

- A személyes és bizalmas felhasználói adatokhoz hozzáférést kibővítő alkalmazásoknak be kell tartaniuk a Google Play hirdetési irányelveit .
- Szükség esetén az adatok szolgáltatóknak történő átvitele jogi okokból is lehetséges (például érvényes kormányzati kérés esetén, illetve a törvényeknek való megfelelés érdekében), vagy ha az átvitel egy cégegyesülés vagy -felvásárlás részét képezi. Ilyen esetben a felhasználókat a törvényeknek megfelelően értesíteni kell.

- Minden személyes és bizalmas felhasználói adatot biztonságosan kell kezelni, amibe beletartozik az is, hogy az adattovábbítás valamilyen modern titkosítással (például HTTPS-protokollal) történjen.
- Az Android-engedélyek által korlátozott adatokhoz való hozzáférés előtt futásidőben küldhető engedélykérést kell alkalmazni (ha lehetséges).
- Nem lehet személyes és bizalmas felhasználói adatokat értékesíteni.
  - Az „értékesítés” személyes és érzékeny felhasználói adatok cseréjét vagy átadását jelenti harmadik félnek pénzbeli ellenérték fejében.
    - A személyes és érzékeny felhasználói adatok felhasználó által kezdeményezett továbbítása (például amikor a felhasználó az alkalmazás egy funkcióját használja arra, hogy fájlt továbbítson egy harmadik félnek, vagy amikor a felhasználó úgy dönt, hogy egy kifejezetten kutatási célú alkalmazást használ) nem minősül értékesítésnek.

A jól látható közlésre és a hozzájárulásra vonatkozó követelmények

Azokban az esetekben, amikor a személyes és érzékeny felhasználói adatok hozzáférése, gyűjtése, felhasználása vagy megosztása az alkalmazásban nem felel meg az adott termék vagy funkció felhasználója észszerű elvárásainak (például ha az adatgyűjtés a háttérben történik, amikor a felhasználó nem használja az alkalmazást), az alábbi követelményeknek kell megfelelned:

Jól látható nyilatkozat: Meg kell jelenítenie az alkalmazáson belül egy nyilatkozatot az adatokhoz való hozzáférésről, valamint azok gyűjtéséről, felhasználásáról és megosztásáról. Az alkalmazáson belüli nyilatkozatnak:

- magában az alkalmazásban kell szerepelnie, nem csak az alkalmazás leírásában vagy valamilyen webhelyen;
- az alkalmazás normál használata során kell megjelennie, és nem követelheti meg a felhasználótól, hogy valamelyik menübe vagy a beállításokba navigáljon;
- meg kell adnia az elért vagy gyűjtött adatok körét;
- ismertetnie kell az adatok felhasználási és megosztási módját;
- nem szabad kizárólag a vonatkozó adatvédelmi irányelvekben vagy az általános szerződési feltételekben szerepelnie; valamint
- nem szabad együtt szerepelnie más, a személyes és bizalmas felhasználói adatok gyűjtésétől eltérő témájú nyilatkozatokkal.

Beleegyezés és futáskor kért engedélyek: az alkalmazáson belüli felhasználói hozzájárulásra vonatkozó és a futáskor kért engedélykérelmeket közvetlenül meg kell előznie egy olyan alkalmazáson belüli nyilatkozatnak, amely megfelel a jelen irányelv követelményeinek. Az alkalmazáson belüli, hozzájárulás megszerzésére irányuló kérelemnek:

- az engedélykérés párbeszédpanelén jól látható és egyértelmű módon kell megjelennie;
- felhasználói műveletet (pl. koppintással elfogadás, jelölőnégyzet bejelölése) kell igényelnie;
- tilos úgy értelmeznie a nyilatkozattól való elnavigálást (pl. a máshová történő koppintást, illetve a Vissza vagy a Kezdőképernyő gomb megnyomását), mint az engedély megadását;
- tilos automatikusan eltűnő vagy lejáró üzeneteket használni a felhasználói hozzájárulás megszerzésének módjaként; és
- a felhasználó engedélyét még azelőtt kell kérni, hogy az alkalmazás megkezdené a személyes és érzékeny felhasználói adatok gyűjtését vagy az ilyen adatokhoz való hozzáférést.

Azoknak az alkalmazásoknak, amelyek más jogalapra (például az EU GDPR szerinti jogos érdekre) támaszkodnak a személyes és érzékeny felhasználói adatok hozzájárulás nélküli feldolgozásához, meg kell felelniük az összes vonatkozó jogszabályi előírásnak, és megfelelő tájékoztatást kell nyújtaniuk a felhasználóknak, beleértve az alkalmazáson belüli tájékoztatást is, ahogyan azt a jelen szabályzat előírja.

A szabályzattal kapcsolatos követelmények teljesítése érdekében javasoljuk az alábbi példa formátumát referenciaként használni a jól látható nyilatkozathoz, amennyiben ez kötelező:

- „[Ez az alkalmazás] [adattípus] típusú adatokat gyűjt/továbbít/szinkronizál/tárol a(z) [„funkció"] engedélyezéséhez, [ilyen esetben]."
- *Példa: „A Fitness Funds helyadatokat gyűjt a fitnesztevékenységek nyomon követéséhez akkor is, ha az alkalmazás nincs megnyitva, illetve nincs használatban, és az adatok a hirdetések támogatására is szolgálnak."*
- *Példa: „A Call buddy olvasási és írási adatokat gyűjt a névjegyek rendezésének támogatásához akkor is, ha az alkalmazás nincs használatban."*

Ha alkalmazásodban olyan, harmadik féltől származó kód (például SDK) szerepel, amelynek célja alapértelmezés szerint a személyes és érzékeny felhasználói adatok gyűjtése, akkor a Google Playtől érkezett kéréstől számított 2 héten belül (vagy ha a Play kérésében ennél hosszabb határidő szerepel, akkor az adott időn belül) megfelelő bizonyítékot kell benyújtanod arra vonatkozóan, hogy az alkalmazásod megfelel az irányelvben szereplő, a jól látható közlésre és a hozzájárulásra vonatkozó követelményeknek, köztük a harmadik fél kódjának segítségével az adatokhoz való hozzáférésre, az adatgyűjtésre, adathasználatra és adatmegosztásra érvényes követelményeknek is.

Néhány példa a gyakori irányelvsértésekre:

- Olyan alkalmazás, amely gyűjti az eszköz helyadatait, de nem rendelkezik jól látható nyilatkozattal, amely elmagyarázza, hogy mely funkció használja ezeket az adatokat és/vagy jelöli az alkalmazás adathasználatát a háttérben.
- Olyan alkalmazás, amely futtatáskor engedélyt kér az adatokhoz való hozzáféréshez, mielőtt megjelenik a jól látható nyilatkozat, amelyben közli, hogy mire használja az adatokat.
- Olyan alkalmazás, amely hozzáfér a felhasználó telepített alkalmazásainak listájához, de ezt nem olyan személyes vagy bizalmas felhasználói adatként kezeli, amelyre vonatkoznak a fenti Adatvédelmi irányelvek, valamint az adatkezelésre és az egyértelmű tájékoztatásra és beleegyezésre vonatkozó követelmények.
- Olyan alkalmazás, amely hozzáfér a felhasználó telefon- vagy címtáradataihoz, de nem olyan személyes vagy bizalmas felhasználói adatokként kezeli őket, amelyekre vonatkoznak a fenti Adatvédelmi irányelvek, valamint az adatkezelésre és az egyértelmű tájékoztatásra és beleegyezésre vonatkozó követelmények.
- Olyan alkalmazás, amely felveszi a felhasználó képernyőjén történteket, és ezeket az adatokat nem kezeli a jelen irányelv hatálya alá tartozó személyes vagy bizalmas adatokként.
- Olyan alkalmazás, amely gyűjti az eszköz helyadatait , és nem ismerteti minden részletre kiterjedően az adatok felhasználását, vagy nem szerez hozzájárulást a fenti követelményeknek megfelelően.
- Olyan alkalmazás, amely az alkalmazás hátterében korlátozott engedélyeket használ (például követési, kutatási és marketingcélokra), és nem ismerteti minden részletre kiterjedően az ilyen adatok felhasználását, vagy nem szerez hozzájárulást a fenti követelményeknek megfelelően.
- Olyan SDK-val rendelkező alkalmazás, amely személyes és érzékeny felhasználói adatokat gyűjt, és ezeket az adatokat nem kezeli úgy, mint amelyek a jelen felhasználói adatokra vonatkozó irányelvek, a hozzáférésnek, az adatkezelésnek (beleértve a tiltott értékesítést), valamint a feltűnő közzétételi és hozzájárulási követelményeknek a hatálya alá tartoznak.

Ebben a cikkben további információ található a jól látható közlésre és a hozzájárulásra vonatkozó követelményekről.

A személyes és bizalmas adatokhoz való hozzáférésre vonatkozó korlátozások

A fent felsorolt követelmények mellett konkrét tevékenységekre vonatkozó követelményeket is meghatározunk, melyeket az alábbi táblázat ismertet.

Tevékenység	Követelmény
Az alkalmazás pénzügyi vagy fizetési adatokat, illetve hatóság által kiállított igazolványokon megtalálható azonosító számokat kezel	Az alkalmazás soha nem tehet nyilvánosan közzé a pénzügyi vagy fizetési tevékenységekkel vagy a hatóságok által kiállított igazolványokon megtalálható azonosító számokkal kapcsolatos semmilyen személyes és bizalmas felhasználói adatot.
Az alkalmazás nem nyilvános telefonkönyvi vagy névjegyadatokat kezel	Nem engedélyezzük személyek nem nyilvános elérhetőségi adatainak jogosulatlan közzétételét vagy átadását.
Az alkalmazás vírusirtó vagy biztonsági funkciókkal (például víruskereső funkcióval, illetve rosszindulatú programok elleni védelemmel vagy biztonsággal kapcsolatos egyéb funkcióval) is rendelkezik	Az alkalmazásnak adatvédelmi irányelveket kell közzétennie, amelyek – az alkalmazáson belüli tájékoztatókkal együtt – ismertetik, hogy az alkalmazás milyen felhasználói adatokat gyűjt és továbbít, valamint hogyan használja fel, és milyen harmadik felekkel osztja meg őket.
Az alkalmazás célközönsége gyermekeket foglal magában	Az alkalmazás nem tartalmazhat olyan SDK-t, amely nincs jóváhagyva gyermekeknek készült szolgáltatásokban való használatra. Az irányelv teljes szövege és a követelmények itt találhatók: Alkalmazások tervezése gyermekek és családok számára .
Az alkalmazás állandó eszközazonosítókat (pl. IMEI, IMSI, SIM-sorozatszám stb.) gyűjt vagy kapcsol össze más adatokkal	Az állandó eszközazonosítók nem kapcsolhatók össze más személyes és bizalmas felhasználói adatokkal vagy visszaállítható eszközazonosítókkal, a következők kivételével: • SIM-alapú azonosításhoz kötődő telefonos szolgáltatások (pl. szolgáltatói fiókkal összekapcsolt Wi-Fi-hívás); • eszköztulajdonosi módot használó vállalati eszközkezelő alkalmazások. Ezeket a felhasználási módokat egyértelműen a felhasználók tudomására kell hozni a felhasználói adatokra vonatkozó irányelveknek megfelelően. Ez a segédanyag bemutatja az egyéb használható egyedi azonosítókat. Az androidos hirdetésazonosítókkal kapcsolatos további útmutatás a hirdetési irányelvekben található.

Adatbiztonsági szakasz

Minden fejlesztőnek egyértelmű és pontos Adatbiztonsági szakaszt kell kitöltenie az összes alkalmazásnál a felhasználói adatok begyűjtésére, felhasználására és megosztására vonatkozóan. A fejlesztő felelős a címke tartalmának pontosságáért, és hogy az információk naprakészek legyenek. Adott esetben az Adatbiztonsági szakasznak konzisztensnek kell lennie az alkalmazás adatvédelmi irányelveiben foglaltakkal.

Lásd ezt a cikket további információkért az Adatbiztonság szakasz kitöltésével kapcsolatban.

Adatvédelmi irányelvek

Minden alkalmazáshoz közzé kell tenni az adatvédelmi irányelvekre mutató linket a Play Console megfelelő mezőjében, továbbá az adatvédelmi irányelvekre mutató linket vagy az adatvédelmi irányelvek szövegét magában az alkalmazásban. Az adatvédelmi irányelveknek az alkalmazáson belüli esetleges adatvédelmi nyilatkozatokkal együtt átfogóan ismertetniük kell, hogy az alkalmazás hogyan fér hozzá a felhasználói adatokhoz, illetve hogyan gyűjti, használja fel és osztja meg őket, az Adatbiztonsági szakaszban közzétett adatokon túl. Idetartoznak többek között az alábbiak:

- fejlesztői információk és adatvédelmi kapcsolattartó vagy a megkeresések benyújtására alkalmas mechanizmus;
- nyilatkozat közzététele arról, hogy az alkalmazás milyen típusú személyes és bizalmas felhasználói adatokhoz fér hozzá, illetve milyen személyes és bizalmas adatokat gyűjt, használ és oszt meg, valamint az esetleges harmadik felekről, akikkel megosztja a személyes vagy bizalmas felhasználói adatokat;
- a személyes és bizalmas felhasználói adatok kezeléséhez alkalmazott biztonságos eljárások;
- a fejlesztő adatmegőrzésre és adatok törlésére vonatkozó irányelvei;
- egyértelmű jelzése annak, hogy adatvédelmi irányelvekről van szó (például az „adatvédelmi irányelvek” megnevezés használata a címben).

Az alkalmazás Google Play-adatlapján megnevezett jogi személyt (például fejlesztőt vagy vállalatot) fel kell tüntetni az alkalmazás adatvédelmi irányelveiben, illetve az alkalmazást meg kell nevezni az adatvédelmi irányelvekben. A személyes és bizalmas felhasználói adatokhoz hozzáféréssel nem rendelkező alkalmazásoknak is be kell küldeniük adatvédelmi irányelveket.

Gondoskodni kell arról, hogy az adatvédelmi irányelvek aktív, nyilvánosan hozzáférhető és geokerítéssel nem védett URL-címen álljanak rendelkezésre (PDF nem megengedett), és hogy ne legyenek szerkeszthetők.

Fióktörlési követelmények

Ha az alkalmazásod lehetőséget biztosít a felhasználóknak arra, hogy fiókot hozzanak létre az alkalmazásodban, akkor azt is lehetővé kell tenned, hogy a felhasználók kérhessék a fiókjuk törlését. A felhasználók számára jól látható módon kell biztosítanod az alkalmazásfiók törlése alkalmazáson belülről és kívülről történő kezdeményezését – például úgy, hogy felkeresik a webhelyedet. Az erre a webes erőforrásra mutató linket a Play Console megfelelő URL-cím űrlapmezőjébe kell beírni.

Az alkalmazásfiók felhasználói kérésre való törlésekor törölnöd kell az adott felhasználó alkalmazásfiókjához társított felhasználói adatokat is. A fiók ideiglenes inaktiválása, letiltása vagy az alkalmazásfiók „befagyasztása” nem minősül a fiók törlésének. Ha indokolt okból – például biztonsági okból, a csalás megelőzése vagy a jogszabályoknak való megfelelés érdekében – meg kell őrizned bizonyos adatokat, akkor egyértelműen tájékoztatnod kell a felhasználókat adatmegőrzési gyakorlatodról (pl. az adatvédelmi irányelveidben).

Ha további információt szeretnél a fióktörlésre vonatkozó irányelv követelményeiről, tekintsd meg ezt a súgócikket. Az Adatbiztonsági űrlap frissítéséről bővebben ebben a cikkben olvashatsz.

Alkalmazáskészlet-azonosító használata

Az Android új azonosítót vezet be az alapvető használati esetek (pl. elemzés és csalásmegelőzés) támogatásához. Az azonosító használatának feltételei alább találhatók.

- **Használat**: Az alkalmazáskészlet-azonosító nem használható hirdetések személyre szabására és mérésére.
- **Személyazonosításra alkalmas adatokkal vagy más azonosítókkal való társítás:** Előfordulhat, hogy az alkalmazásban beállított azonosítót nem lehet csatlakoztatni valamilyen Android-azonosítóhoz (például Android-hirdetésazonosítóhoz, AAID), vagy személyes és bizalmas adatok hirdetése céljából.
- **Átláthatóság és beleegyezés**: Az alkalmazásban beállított azonosító gyűjtését és használatát, valamint jelen szerződési feltételek betartását a jogszabályoknak megfelelő adatvédelmi értesítésben kell tudatni a felhasználókkal, ideértve a saját adatvédelmi irányelveidet is. Szükség szerint be kell szerezni a felhasználók jogilag érvényes hozzájárulását. Az adatvédelmi alapelveinkről a felhasználói adatokra vonatkozó irányelvünk nyújt további tájékoztatást.

EU-U.S., Swiss Privacy Shield (EU–USA és Svájc–USA adatvédelmi pajzs)

Ha olyan személyes adatokhoz fér hozzá, használ vagy dolgoz fel, amelyeket a Google tett hozzáférhetővé, és amelyek közvetlenül vagy közvetve személyek azonosításához használhatók, továbbá az Európai Unióból vagy Svájcból származnak („EU-s személyes adatok”), akkor:

- meg kell felelnie valamennyi vonatkozó, a magánélet védelmével foglalkozó, adatvédelmi és adatbiztonsági jogszabálynak, irányelvnek, rendeletnek és szabálynak;
- az EU-s személyes adatokhoz való hozzáférés, továbbá az EU-s személyes adatok felhasználása vagy feldolgozása kizárólag olyan céllal történhet, amely összhangban áll annak a személynek a beleegyezésével, akihez az EU-s személyes adatok kapcsolódnak;
- megfelelő szervezeti és műszaki intézkedéseket kell megvalósítania, amelyek biztosítják az EU-s személyes adatok elvesztéssel, helytelen használattal, jogosulatlan vagy jogsértő hozzáféréssel, nyilvánosságra hozatallal, megváltoztatással és megsemmisüléssel szembeni védelmét; és
- ugyanolyan szintű védelmet kell biztosítania, mint amelyet az adatvédelmi pajzs előírásai megkövetelnek.

Az e feltételeknek való megfelelést rendszeresen ellenőrizni kell. Ha a fejlesztő nem tudja teljesíteni ezeket a feltételeket (vagy ha jelentős kockázata van annak, hogy nem tudja teljesíteni őket), akkor azonnal értesítenie kell bennünket e-mailben a data-protection-office@google.com címen, és vagy azonnal fel kell hagynia az EU-s személyes adatok feldolgozásával, vagy észszerű és megfelelő lépéseket kell tennie annak érdekében, hogy visszaállítsa a szükséges kívánalmaknak megfelelő védelmi szintet.

2020. július 16-tól a Google már nem az EU-U.S. Privacy Shield (EU–USA adatvédelmi pajzs) keretrendszerre hagyatkozik olyan személyes adatok továbbítása esetén, amelyek az EGT-ből vagy az Egyesült Királyságból az USA-ba kerülnek továbbításra. (További információ.)További információt a Fejlesztői terjesztési megállapodás 9. szakaszában talál.

Engedélyek és bizalmas információhoz hozzáférő API-k

Az engedély- és a bizalmas információkhoz hozzáférő API-kéréseket közérthető módon kell megfogalmazni a felhasználó számára. Csak olyan engedélyeket és bizalmas információkhoz hozzáférő API-kat kérhetsz, amelyek az alkalmazás meglévő, Google Play-adatlapján ismertetett funkcióinak vagy szolgáltatásainak megvalósításához szükségesek. Nem használhatsz sem olyan engedélyeket, sem olyan bizalmas információkhoz hozzáférő API-kat, amelyek nem nyilvános, megvalósításra nem kerülő vagy nem engedélyezett funkciókhoz vagy célokra biztosítanak hozzáférést a felhasználói vagy eszközadatokhoz. Az engedélyeknek vagy a bizalmas információkhoz hozzáférő API-knak köszönhetően megismert személyes vagy bizalmas adatok értékesítése, illetve értékesítési célból történő megosztása tilos.

Az adatokhoz való hozzáféréshez szükséges engedély- és a bizalmas információkhoz hozzáférő API-kéréseket összefüggéseiben, fokozatosan jelezd, hogy a felhasználó megértse, miért kér engedélyt az alkalmazás. Az adatok csak olyan célokra használhatók, amelyekhez a felhasználók hozzájárulásukat adták. Ha a fejlesztő később más célokra szeretné használni az adatokat, meg kell kérdeznie a felhasználókat, és gondoskodnia kell arról, hogy egyértelműen kifejezzék hozzájárulásukat az adatok további felhasználási módjaihoz.

Korlátozott engedélyek

A fentiek mellett a korlátozott engedélyek olyan engedélyek, amelyek veszélyesként , speciálisként , jellegzetesként , illetve az alábbiak szerint vannak meghatározva. Ezekre az engedélyekre a következő kiegészítő követelmények és korlátozások is érvényesek:

- A Korlátozott Engedélyek segítségével elért felhasználói vagy eszközadatok személyes és érzékeny felhasználói adatoknak minősülnek. Az ilyen adatokra a Felhasználói adatokra vonatkozó irányelvek vonatkoznak.
- Ha a felhasználó elutasítja a korlátozott engedélyre vonatkozó kérést, tiszteletben kell tartani a döntését, emellett a felhasználókat nem lehet úgy manipulálni, illetve arra kényszeríteni, hogy

elfogadjanak nem alapvető fontosságú engedélyeket. A fejlesztőknek észszerű keretek között lehetőséget kell biztosítaniuk azon felhasználóknak is az alkalmazás használatára, akik nem járulnak hozzá a bizalmas engedélyek használatához (pl. ha a felhasználó korlátozta a hívásnaplóhoz való hozzáférést, akkor lehetőséget kell neki adni a telefonszámok manuális bevitelére).

- Kimondottan tilos az engedélynek a Google Play rosszindulatú programokra vonatkozó irányelveivel (beleértve az magasabb szintű jogosultságokkal való visszaélésre vonatkozó irányelvvel) ellentétes módon történő felhasználása.

Egyes korlátozott engedélyekre az alább részletezett további követelmények is érvényesek lehetnek. E korlátozások célja a felhasználói adatok védelme. Korlátozott kivételeket biztosíthatunk e követelmények alól azokban az igen ritka esetekben, amikor az adott alkalmazás valamilyen rendkívül lenyűgöző vagy nagyon fontos funkcióval rendelkezik, és a funkció biztosítására pillanatnyilag nincs más módszer. A kivételkéréseket a felhasználókra gyakorolt lehetséges biztonsági vagy adatvédelmi hatásokat figyelembe véve mérlegeljük.

SMS-re és hívásnaplóra vonatkozó engedélyek

Az SMS-sel és a hívásnaplóval kapcsolatos engedélyek személyes és bizalmas felhasználói adatoknak minősülnek, amelyekre a személyes és bizalmas adatokra vonatkozó irányelv és a következő korlátozások érvényesek:

Korlátozott engedély	Követelmény
Hívásnapló engedélycsoport (pl. READ_CALL_LOG, WRITE_CALL_LOG, PROCESS_OUTGOING_CALLS)	Alapértelmezett telefon- vagy segédkezelőként aktívan regisztrálva kell lennie az eszközön.
SMS engedélycsoport (pl. READ_SMS, SEND_SMS, WRITE_SMS, RECEIVE_SMS, RECEIVE_WAP_PUSH, RECEIVE_MMS)	Alapértelmezett SMS- vagy segédkezelőként aktívan regisztrálva kell lennie az eszközön.

Azok az alkalmazások, amelyek nem rendelkeznek alapértelmezett SMS-, telefon- vagy segédkezelői képességgel, nem deklarálhatják a fenti engedélyek használatát a manifest fájlban. Ide tartozik a manifestben szereplő helyőrző szöveg is. Emellett minden alkalmazásnak alapértelmezett SMS-, telefon- vagy segédkezelőnek kell lennie, mielőtt a felhasználót a fenti engedélyek bármelyikének elfogadására kérné, és haladéktalanul meg kell szakítania az engedély használatát, ha már nem alapértelmezett kezelő. Az engedélyezett használatról és a kivételekről szóló tájékoztatás ebben a súgócikkben található.

Az alkalmazások az engedélyt (és az engedélyből származó minden adatot) csak az alkalmazás jóváhagyott és alapvető funkcióinak biztosítására használhatják. Az alapvető funkció az alkalmazás elsődleges célját jelenti. Az elsődleges cél állhat több alapvető funkcióból is, melyek mindegyikét dokumentálni és jól láthatóan jelezni kell az alkalmazás leírásában. Az alapvető funkciók nélkül az alkalmazás „elromlik”, illetve nem használható. Az adatok továbbítására, megosztására vagy engedéllyel történő használatára csak az alkalmazáson belüli alapvető funkciók vagy szolgáltatások biztosítása érdekében van lehetőség, és használatuk ettől eltérő célra nem terjeszthető ki (például más alkalmazások vagy szolgáltatások javítására, illetve hirdetési vagy marketingcélokra). Nem használhatók alternatív megoldások (például más engedélyek, API-k vagy harmadik féltől származó források) a hívásnapló- vagy SMS-engedélyekhez társított adatok kinyerésére.

Helymeghatározási jogosultságok

Az Eszköz helye személyes és bizalmas felhasználói adatnak minősül, amelyre a személyes és bizalmas adatokra vonatkozó irányelvek, a háttérbeli helyadatok irányelve és a következő követelmények vonatkoznak:

- Az alkalmazások nem férhetnek hozzá olyan adatokhoz, amelyeket helymeghatározási engedélyek védenek (pl. ACCESS_FINE_LOCATION, ACCESS_COARSE_LOCATION,

ACCESS_BACKGROUND_LOCATION), ha már nincs szükség rájuk az alkalmazás meglévő funkcióinak vagy szolgáltatásainak biztosításához.

- Soha ne kérjen helymeghatározási jogosultságokat a felhasználóktól kizárólag hirdetési vagy elemzési célból. Azoknak az alkalmazásoknak, amelyek kiterjesztik az ilyen adatok megengedett felhasználhatóságát hirdetések megjelenítésére, meg kell felelniük a hirdetési irányelveknek .
- Az alkalmazásoknak a lehető legkisebb hatókört kell kérniük (azaz nem pontos, hanem hozzávetőleges adatokat, és az előtérben, nem a háttérben), amely ahhoz szükséges, hogy biztosítani tudják a helymeghatározást igénylő meglévő funkciót vagy szolgáltatást, és a felhasználók számára észszerűen elvárható kell legyen, hogy a helyadatok igényelt szintjére szüksége van az adott funkciónak vagy szolgáltatásnak. Elutasíthatjuk például azokat az alkalmazásokat, amelyek meggyőző indok nélkül kérnek vagy valósítanak meg hozzáférést a háttérbeli helyadatokhoz.
- A háttérbeli helyhozzáférés csak arra használható, hogy az alkalmazás alapvető működéséhez kapcsolódó, a felhasználók számára előnyös funkciókat biztosítsanak.

Az alkalmazások hozzáférhetnek a tartózkodási helyhez előtérben futó szolgáltatásra vonatkozó engedély használatával (amikor az alkalmazás csak előtérbeli hozzáféréssel rendelkezik; például: „használat közben”), ha a felhasználás:

- kezdeményezése az alkalmazáson belül, a felhasználó által indított művelet folytatásaként valósul meg; és
- azonnal véget ér, amint az alkalmazás befejezi a felhasználó által indított művelethez kapcsolódó használatot.

A kifejezetten gyermekeknek szóló alkalmazásoknak meg kell felelniük Az egész családnak program irányelveinek.

Az irányelv követelményeiről ebben a súgócikkben található további információ.

A „Hozzáférés minden fájlhoz” engedély

A felhasználó eszközén található fájlok és könyvtárak attribútumai személyes és bizalmas felhasználói adatnak minősülnek, amelyekre a személyes és bizalmas adatokra vonatkozó irányelv és a következő követelmények érvényesek:

- Az alkalmazások csak akkor kérhetnek hozzáférést az eszköztárhelyhez, ha elengedhetetlen az alkalmazás működéséhez, és nem kérhetnek hozzáférést az eszköztárhelyhez harmadik fél nevében olyan célból, amely nem kapcsolódik a felhasználók számára nyújtott alapvető alkalmazásfunkciókhoz.
- Az Android R vagy újabb verzióját futtató eszközöknél a MANAGE_EXTERNAL_STORAGE engedélyre van szükség a megosztott tárhelyhez kapcsolódó hozzáférés kezeléséhez. Az R verziót célzó és a megosztott tárhelyre vonatkozó széles körű hozzáférést („Hozzáférés minden fájlhoz”) kérő alkalmazásoknak az alkalmazás közzététele előtt sikeresen teljesíteniük kell a megfelelő hozzáférési ellenőrzést. Az engedély használatára jogosult alkalmazásoknak egyértelműen kérniük kell a felhasználókat, hogy engedélyezzék az alkalmazás „Hozzáférés minden fájlhoz” beállítását a „Különleges alkalmazás-hozzáférés” szakaszban. Az Android R követelményeiről ebben a súgócikkben találhat további információt.

Csomagra (alkalmazás) vonatkozó láthatósági engedélyek

A bármely eszközről lekérdezett telepített alkalmazások készlete személyes és bizalmas felhasználói adatnak minősül, amelyre a személyes és bizalmas adatokra vonatkozó irányelv és az alábbi követelmények érvényesek.

Azok az alkalmazások, amelyeknek alapvető rendeltetése az eszközön található más alkalmazások elindítása, keresése vagy a velük való együttműködés, az engedély hatáskörének megfelelő láthatóságot kaphatnak az eszközön található egyéb telepített alkalmazásokhoz az alábbiak szerint:

- **Alkalmazások általános láthatósága:** Általános láthatóság esetén az alkalmazás széleskörű (vagy „általános”) láthatósággal rendelkezik az eszközön lévő telepített alkalmazásokhoz („csomagok”).
  - A 30-as vagy újabb API-szintet célzó alkalmazások esetén a telepített alkalmazásokhoz a QUERY_ALL_PACKAGES engedélyen keresztül biztosított általános láthatóság meghatározott használati esetekre korlátozódik, amelyeknél az alkalmazás működéséhez szükség van az eszközön található alkalmazások ismeretére és a velük való kompatibilitásra.
    - Nem használhatja a QUERY_ALL_PACKAGES engedélyt, ha az alkalmazás célzottabb hatókörű csomagláthatósági nyilatkozattal is tud működni (pl. általános láthatóság kérése helyett konkrét csomagok lekérdezése és használata).
  - Az alternatív módszerek használata a QUERY_ALL_PACKAGES engedélyhez kapcsolódó általános láthatósági szint megközelítéséhez szintén az alkalmazás felhasználók számára megjelenő, alapvető funkciójára és az ilyen módszerrel felfedezett alkalmazásokkal való kompatibilitásra korlátozódik.
  - Ebben a súgócikkben tájékozódhat a QUERY_ALL_PACKAGES engedély megengedhető használati eseteiről.
- **Alkalmazások korlátozott láthatósága**: A korlátozott láthatóság azt jelenti, hogy az alkalmazás minimálisra csökkenti az adatokhoz való hozzáférést azáltal, hogy „általános” helyett célzottabb módszerekkel kérdezi le a konkrét alkalmazásokat (pl. olyan konkrét alkalmazásokat keres, amelyek megfelelnek az alkalmazás manifestnyilatkozatának). Ez a módszer használható arra, hogy alkalmazásokat kérdezzen le olyan esetekben, amikor az alkalmazás az irányelveknek megfelelő kompatibilitással vagy ezen alkalmazások feletti felügyelettel rendelkezik.
- Az eszközön található telepített alkalmazások készlete láthatóságának közvetlenül kapcsolódnia kell ahhoz az alapvető célhoz vagy alapvető funkcióhoz, amelyhez a felhasználók hozzáférnek az alkalmazáson belül.

A Playen keresztül terjesztett alkalmazásokból lekérdezett, alkalmazáskészletekkel kapcsolatos adatokat tilos értékesíteni vagy megosztani elemzés vagy hirdetésekből származó bevételszerzés céljából.

Accessibility API

Az Accessibility API-t nem lehet a következőkre használni:

- felhasználói beállítások engedély nélküli módosítása, illetve annak a lehetőségnek a megakadályozása, hogy a felhasználó letiltson vagy eltávolítson bármilyen alkalmazást vagy szolgáltatást, kivéve, ha a szülő vagy gyám ezt engedélyezi egy szülőifelügyelet-alkalmazáson keresztül, vagy ha ezt erre jogosult rendszergazda engedélyezi vállalatirányítási rendszeren keresztül;
- az Android rendszer beépített adatvédelmi beállításainak és értesítéseinek megkerülése; vagy
- a felhasználói felület megváltoztatása vagy kihasználása olyan módon, amely megtévesztő, vagy más módon sérti a Google Play fejlesztői irányelveket.

Az Accessibility API-t nem arra tervezték, hogy távoli hívásról hangfelvételt készítsenek vele, illetve nincs mód erre lehetőséget kérni.

Az Accessibility API használatát jelezni kell a Google Play-adatlapon.

Az IsAccessibilityTool eszközre vonatkozó irányelvek

Az olyan alkalmazások, amelyek alapvető funkciói a fogyatékossággal élők közvetlen támogatását szolgálják, jogosultak az **IsAccessibilityTool** használatára annak érdekében, hogy megfelelő módon sorolhassák be magukat akadálymentes alkalmazásként a nyilvános oldalakon.

Azoknak az alkalmazásoknak, amelyek nem jogosultak az **IsAccessibilityTool** használatára, meg kell felelniük a jól látható helyen elhelyezett nyilatkozatra és hozzájárulásra vonatkozó követelményeknek a felhasználói adatokra vonatkozó irányelv értelmében, mivel a kisegítő lehetőségekkel kapcsolatos

funkcióik nem nyilvánvalóak a felhasználó számára. Erről bővebben az AccessibilityService API súgócikkében olvashatsz.

Az alkalmazásoknak a kívánt funkciók eléréséhez lehetőség szerint pontosabban megjelölt API-kat és engedélyeket kell használniuk az Accessiblity API helyett.

Csomagtelepítési engedély kérése

A REQUEST_INSTALL_PACKAGES engedély segítségével egy alkalmazás kérheti alkalmazáscsomagok telepítését. Az engedély használatához az alkalmazásod alapvető funkciói közé kell tartozniuk az alábbiaknak:

- alkalmazáscsomagok küldése vagy fogadása, illetve
- az alkalmazáscsomag felhasználó által kezdeményezett telepítésének engedélyezése.

Az engedélyezett funkciók az alábbiak:

- böngészés vagy keresés;
- a mellékleteket támogató kommunikációs szolgáltatások;
- fájlmegosztás, -továbbítás vagy -kezelés;
- vállalatieszköz-kezelés;
- biztonsági mentés és helyreállítás;
- eszközáttelepítés/telefonátvitel;
- telefon és hordható eszköz vagy IoT-eszköz (például: okosóra vagy okostévé) szinkronizálására használatos társalkalmazás.

Alapvető működésnek az alkalmazás elsődleges célját tekintjük. Az alapvető működést, valamint az alapvető működéshez tartozó összes alapvető funkciót dokumentálni és jól láthatóan jelezni kell az alkalmazás leírásában.

A REQUEST_INSTALL_PACKAGES engedély nem használható önfrissítések, módosítások elvégzésére, illetve az eszközfájlban található egyéb APK-k becsomagolására, kivéve, ha eszközkezelési célokról van szó. Minden frissítésnek és csomagtelepítésnek meg kell felelnie a Google Play Eszközzel és hálózattal való visszaélésről szóló irányelvének, illetve a frissítéseket és telepítéseket a felhasználónak kell kezdeményeznie és végrehajtania.

Health Connect by Android-engedélyek

A Health Connect egy olyan Android-platform, amely lehetővé teszi az egészségügyi és fitneszalkalmazások számára, hogy ugyanazokat az eszközön tárolt adatokat egy egységes ökoszisztémán belül tárolják és osszák meg. Egyúttal olyan egységes helyként is szolgál a felhasználók számára, ahol szabályozni tudják, hogy mely alkalmazások olvashatják és írhatják az egészségügyi és fitneszadatokat. A Health Connect számos különféle adattípus olvasását és írását támogatja, a lépésszámoktól a testhőmérsékletig.

A Health Connect-engedélyek révén elért adatok a felhasználói adatokra vonatkozó irányelvek szerinti személyes és érzékeny felhasználói adatnak minősülnek. Ha az alkalmazásod egészségügyi alkalmazásnak minősül, vagy egészségügyi funkciói vannak és egészségügyi adatokhoz – ideértve a Health Connect-adatokat is – fér hozzá, meg kell felelnie az egészségügyi alkalmazásokra vonatkozó irányelveknek is.

A Health Connect használatával kapcsolatos kezdő lépéseket illetően tájékozódj ebből az Android-fejlesztői útmutatóból. A Health Connect adattípusaihoz való hozzáférés kérelmezésével kapcsolatban lásd ezt a cikket.

A Google Playen terjesztett alkalmazásoknak meg kell felelniük az alábbi irányelvi követelményeknek ahhoz, hogy Health Connect-adatokat olvashassanak és/vagy írhassanak.

Indokolt hozzáférés a Health Connect-adatokhoz és ezek indokolt használata

A Health Connect kizárólag a vonatkozó irányelvekkel, általános szerződési feltételekkel összhangban, továbbá az ebben az irányelvben megállapított, jóváhagyott használati esetek céljára használható. Ez azt jelenti, hogy kizárólag akkor kérhetsz hozzáférést az engedélyekhez, ha alkalmazásod vagy szolgáltatásod megfelel a jóváhagyott használati esetek valamelyikének.

A jóváhagyott használati esetek többek között a következők: fittség és jóllét, jutalmak, fitnesztanácsadás, vállalati jóllét, orvosi ellátás, egészségügyi kutatás és játékok.

Csak olyan alkalmazások vagy szolgáltatások kérhetnek hozzáférést a Health Connect-engedélyekhez, amelyek egy vagy több olyan funkcióval rendelkeznek, amelyek célja a felhasználók egészségének és fittségének javítása. Ezek közé tartoznak a következők:

- Olyan alkalmazások vagy szolgáltatások, amelyek lehetővé teszik a felhasználók számára, hogy **közvetlenül naplózzák, jelentsék, nyomon kövessék és/vagy elemezzék** testmozgásukat, alvásukat, mentális jóllétüket, táplálkozásukat, egészségükkel kapcsolatos mérési adataikat, testi állapotuk leírását és/vagy más, az egészséggel vagy erőnléttel kapcsolatos leírásokat és méréseket.
- Olyan alkalmazások vagy szolgáltatások, amelyek lehetővé teszik a felhasználók számára, hogy az eszközükön **tárolják testmozgásukat, alvásukat, mentális jóllétüket, táplálkozásukat, egészségükkel kapcsolatos mérési adataikat, testi állapotuk leírását** és/vagy más, az egészséggel vagy erőnléttel kapcsolatos leírásokat és méréseket.

A Health Connecthez való hozzáférés nem használható a jelen irányelvet vagy a Health Connectre vonatkozó egyéb általános szerződési feltételeket vagy irányelveket sértő módon, így a következő célokra sem:

- Nem használható a Health Connect olyan alkalmazások, környezetek vagy tevékenységek fejlesztéséhez (vagy olyan alkalmazásokba, környezetekbe vagy tevékenységekbe való beépítés céljára), amelyek esetében a Health Connect használata vagy meghibásodása észszerűen feltételezhető módon vezethet halálhoz, személyi sérüléshez, környezeti vagy anyagi kárhoz (így például nem használható nukleáris létesítmények, légiforgalmi irányító rendszerek, életfenntartó rendszerek vagy fegyverrendszerek létrehozásához vagy működtetéséhez).
- Grafikus felhasználói felület nélküli alkalmazásokkal nem megengedett hozzáférni a Health Connecten keresztül megszerzett adatokhoz. Az alkalmazásoknak egyértelműen azonosítható ikont kell megjeleníteniük az alkalmazástálcán, az eszköz alkalmazásbeállításai között, az értesítési felületen és minden egyéb hasonló területen.
- Nem használható a Health Connect olyan alkalmazásokkal, amelyek inkompatibilis eszközök vagy platformok között szinkronizálják az adatokat.
- Nem használható a Health Connect olyan alkalmazásokhoz, szolgáltatásokhoz vagy funkciókhoz való csatlakozásra, amelyek kizárólag gyermekeket céloznak meg.
- A Health Connect platformot használó valamennyi alkalmazásnak vagy rendszernek a jogosulatlan vagy jogellenes hozzáféréssel, felhasználással, megsemmisítéssel, elvesztéssel, módosítással vagy közléssel szembeni védelmére szolgáló, észszerű és megfelelő lépéseket kell tenned.

Szintén a te feladatod biztosítani a Health Connect, illetve a kapcsolódó platformból származó valamennyi adat tervezett felhasználása alapján esetlegesen alkalmazandó szabályozási vagy jogi előírásoknak való megfelelést. Amennyiben azt a Google által az egyes Google-termékekhez vagy -szolgáltatásokhoz biztosított címke vagy tájékoztató kifejezetten nem jelzi, a Google a Health Connectben szereplő adatok semmilyen felhasználásra vagy célra – és különösen nem kutatási, egészségügyi vagy gyógyászati célra – való alkalmazását nem látja el ajánlásával, és nem is szavatolja az ilyen adatok pontosságát. A Google kizár minden felelősséget a Health Connecten keresztül szerzett adatok felhasználásával kapcsolatban.

Korlátozott használat

A Health Connect használata során az adatokhoz való hozzáférésnek és az adatok felhasználásának meghatározott korlátozásokhoz kell igazodnia:

- Az adatok felhasználásának az alkalmazás kezelőfelületén látható megfelelő felhasználási eset vagy funkciók biztosítására vagy javítására kell korlátozódnia.
- A felhasználói adatok csak a felhasználó kifejezett beleegyezésével továbbíthatók harmadik félnek: biztonsági célból (például visszaélések kivizsgálása céljából), a vonatkozó jogszabályoknak vagy előírásoknak való megfelelés érdekében, vagy fúzió/felvásárlás részeként.
- A felhasználói adatokhoz való emberi hozzáférés korlátozott, kivéve, ha ehhez megtörtént a felhasználó kifejezett beleegyezésének megszerzése, illetve ha az emberi hozzáférés biztonsági célból, a jogszabályoknak való megfelelés érdekében történik, vagy pedig ha a felhasználói adatok a jogi előírásoknak megfelelően a belső műveletek elvégzése céljára összesített formában vannak.
- **A Health Connect-adatok minden más egyéb átadása, felhasználása és értékesítése tilos, ideértve a következőket:**
  - A felhasználói adatok harmadik fél, így például hirdetési platform, adatbróker vagy bármilyen információ-viszonteladó részére történő átadása vagy értékesítése.
  - A felhasználói adatok hirdetések, többek között személyre szabott vagy érdeklődésen alapuló hirdetések megjelenítése céljából történő átadása, értékesítése vagy felhasználása.
  - A felhasználói adatoknak a hitelképesség megállapítása vagy hitelezés céljára való átadása, értékesítése vagy felhasználása.
  - A felhasználói adatok átadása, értékesítése vagy felhasználása olyan termékkel vagy szolgáltatással együtt, amely orvostechnikai eszköznek minősülhet, kivéve, ha az orvostechnikai eszközalkalmazás megfelel minden vonatkozó szabályozásnak, ami azt is magában foglalja, hogy rendelkezik az illetékes szabályozó hatóságok (pl. az USA-ban az FDA) által kibocsátott engedélyekkel és jóváhagyásokkal a Health Connect-adatok tervezett használatát illetően, és a felhasználó kifejezett hozzájárulását adta az adatai ilyen célra történő felhasználásához.
  - A felhasználói adatoknak (a HIPAA meghatározása szerinti) védett egészségügyi adatokat érintő célra vagy módon történő átadása, értékesítése vagy felhasználása, kivéve, ha a Google előzetesen írásban jóváhagyja az ilyen felhasználást.

A hatókör minimalizálása

Csak olyan engedélyekhez szabad hozzáférést kérned, amelyek a termék funkcióinak vagy szolgáltatásainak implementálásához szükségesek. Az ilyen hozzáférési kéréseknek célzottnak és a szükséges adatokra korlátozottaknak kell lenniük.

Átlátható és pontos értesítés és vezérlés

A Health Connect kezeli az egészségügyi és fitneszadatokat, beleértve a bizalmas információkat is, és minden alkalmazástól megköveteli, hogy átfogó adatvédelmi irányelvekkel rendelkezzen. Az adatvédelmi irányelveknek átlátható módon közölniük kell, hogy az alkalmazás hogyan gyűjti, használja és osztja meg a felhasználói adatokat. A jogi előírásokon túl a fejlesztőknek a következő információkat kell feltüntetniük az adatvédelmi irányelvekben:

- pontosan meg kell jeleníteni az alkalmazás identitását, ismertetve az elért adatokat és azok kapcsolatát az alkalmazás jól látható funkcióival vagy ajánlásaival;
- adatmegőrzési és -törlési gyakorlatok;
- adatkezelési eljárások. Például a modern kriptográfia segítségével történő továbbítás (például HTTPS-en keresztül).

Az adatok biztonságos kezelése

Valamennyi felhasználói adatot biztonságosan kell kezelned. A Health Connect platformot használó valamennyi alkalmazásnak vagy rendszernek a jogosulatlan vagy jogellenes hozzáféréssel, felhasználással, megsemmisítéssel, elvesztéssel, módosítással vagy közléssel szembeni védelmére szolgáló, észszerű és megfelelő lépéseket kell tenned.

Az ajánlott biztonsági gyakorlatok közé tartozik az ISO/IEC 27001 szabványban ismertetett információbiztonsági irányítási rendszer bevezetése és fenntartása, valamint annak biztosítása, hogy

az alkalmazás vagy webes szolgáltatás robusztus kialakítású, és az OWASP Top 10 által meghatározott általános biztonsági problémáktól mentes legyen.

A használatban lévő API-tól és a felhasználói engedélyek vagy a felhasználók számától függően megköveteljük, hogy amennyiben terméked a felhasználó saját eszközén kívülre továbbít adatokat, alkalmazásod vagy szolgáltatásod egy kijelölt harmadik fél által végzett időszakos biztonsági értékelésen essen át, és erről a harmadik féltől értékelő bizonyítványt kapjon.

A Health Connecthez csatlakozó alkalmazásokra vonatkozó követelményekkel kapcsolatos további információt ebben a súgócikkben találhatsz.

VPN-szolgáltatás

A VpnService olyan alaposztály, amellyel az alkalmazások saját VPN-megoldásokat bővíthetnek és építhetnek. Csak azok az alkalmazások hozhatnak létre biztonságos, eszközszintű alagutat valamely távoli szerverhez, amelyek a VpnService-t használják, és a VPN az alapvető funkciójuk. A kivételek közé tartoznak azok az alkalmazások, amelyek alapvető funkciójukhoz távoli szervert igényelnek, így például a következők:

- szülői felügyeleti és vállalatirányítási funkciójú alkalmazások;
- alkalmazáshasználatot nyomon követő alkalmazások;
- eszközbiztonsági alkalmazások (például vírusirtó, mobileszközök kezelésére szolgáló, tűzfalalkalmazás);
- hálózattal kapcsolatos eszközök (például a távoli hozzáférés);
- böngészőalkalmazások;
- szolgáltatói alkalmazások, amelyek VPN-funkció használatát igénylik a telefonos vagy csatlakozási szolgáltatások biztosításához.

A VpnService nem használható a következőre:

- személyes és érzékeny felhasználói adatok gyűjtése jól látható nyilatkozat és beleegyezés nélkül;
- az eszközön lévő más alkalmazások felhasználói forgalmának átirányítása vagy manipulálása bevételszerzési céllal (például hirdetési forgalom átirányítása a felhasználóétól eltérő országon keresztül);

A VpnService szolgáltatást használó alkalmazásoknak:

- dokumentálniuk kell a VpnService használatát a Google Play-adatlapon, és
- az eszköztől a VPN-alagút végpontjáig titkosítaniuk kell az adatokat, és
- meg kell felelniük valamennyi Fejlesztői programszabályzatnak, köztük a hirdetési csalással, az engedélyekkel és a rosszindulatú szoftverekkel kapcsolatos irányelveknek.

Pontos ébresztő jogosultság

Új engedély, a USE_EXACT_ALARM bevezetésére kerül majd sor: ez az engedély az Android 13-tól kezdődően hozzáférést nyújt majd az alkalmazásokban a pontos ébresztés funkcióhoz (a 33-as API szintet célzó alkalmazások).

A USE_EXACT_ALARM korlátozott engedély, az alkalmazásoknak pedig csak akkor kell deklarálniuk ezt az engedélyt, ha az alapvető funkciójuk támogatja a pontos ébresztés szükségességét. Az ezt a korlátozott engedélyt kérelmező alkalmazásokat felülvizsgálat terheli, és amelyikük nem felel meg az elfogadható használati esettel kapcsolatos feltételeknek, annak a Google Playen való közzététele nem lesz engedélyezve.

A Pontos ébresztés engedély elfogadható használati esetei

Alkalmazásod csak olyankor használhatja a USE_EXACT_ALARM funkciót, amikor az alkalmazásod alapvető, a felhasználók számára biztosított funkciója pontosan időzített műveletet igényel, azaz, ha:

- az alkalmazás ébresztő vagy időzítő alkalmazás;

- az alkalmazás naptáralkalmazás, amely eseményekkel kapcsolatos értesítéseket jelenít meg;

ha a pontos értesítő funkció olyan esetével rendelkezik, amelyet nem fed le a fentiek valamelyike, akkor azt kell eldöntened, hogy a SCHEDULE_EXACT_ALARM alternatívaként való használata opció lehet-e.

A pontos ébresztés funkcióval kapcsolatos további információt ebben a fejlesztői iránymutatásban találsz.

Teljes képernyős intentengedély

Az Android 14-et (megcélzott API-szint: 34) vagy újabb verziót célzó alkalmazásoknál a USE_FULL_SCREEN_INTENT egy speciális alkalmazás-hozzáférési engedély . Az alkalmazások csak akkor kapják meg automatikusan a USE_FULL_SCREEN_INTENT engedélyt, ha az alkalmazás alapvető funkciója az alábbi olyan kategóriák valamelyikébe esik, melyeknek magas prioritású értesítésekre van szükségük:

- ébresztő beállítása;
- telefon- vagy videohívások fogadása.

Az ezt az engedélyt kérelmező alkalmazások felülvizsgálaton esnek át, és amelyikük nem felel meg a fenti feltételeknek, az nem kapja meg automatikusan ezt az engedélyt. Ilyen esetben az alkalmazásoknak engedélyt kell kérniük a felhasználótól a USE_FULL_SCREEN_INTENT használatára.

Szeretnénk emlékeztetni arra**,** hogy a USE_FULL_SCREEN_INTENT engedély mindennemű használatának meg kell felelnie a Google Play fejlesztői irányelveknek, beleértve a nemkívánatos mobilszoftverekre, az eszközzel és a hálózattal való visszaélésekre és a hirdetésekre vonatkozó irányelveket is. A teljes képernyős intentértesítések nem akadályozhatják, nem zavarhatják, illetve nem károsíthatják a felhasználó eszközét, és nem férhetnek hozzá jogosulatlanul. Emellett az alkalmazások nem zavarhatják sem a többi alkalmazást, sem az eszköz használhatóságát.

A USE_FULL_SCREEN_INTENT engedélyről további információ található a Súgóban.

Eszközzel és hálózattal való visszaélés

Nem engedélyezzük azokat az alkalmazásokat, amelyek jogosulatlan módon zavarják, akadályozzák, károsítják vagy érik el a felhasználó eszközét, illetve más eszközöket, számítógépeket, szervereket, hálózatokat, alkalmazásprogramozási felületeket (API-kat) vagy szolgáltatásokat, köztük az eszközön megtalálható egyéb alkalmazásokat, valamilyen Google-szolgáltatást vagy hitelesített szolgáltatói hálózatot.

A Google Play szolgáltatáson keresztül közzétett alkalmazásoknak meg kell felelniük az Android rendszer alapértelmezett optimalizációs követelményeinek, melyek a Core App Quality guidelines for Google Play (Alapvető alkalmazásminőségi irányelvek a Google Play számára) című dokumentumban találhatók.

A Google Playen keresztül terjesztett alkalmazások nem módosíthatják, cserélhetik le vagy frissíthetik saját magukat a Google Play frissítési mechanizmusától eltérő módszerek használatával. Az alkalmazások ugyanígy nem tölthetnek le futtatható kódot sem (például .dex, JAR és hasonló fájlokat) Google Playen kívüli forrásból. A korlátozás nem vonatkozik a virtuális gépen vagy tolmácson futó, az Android API-khoz közvetett hozzáférést biztosító kódokra (például WebView környezetben vagy böngészőben lévő JavaScriptre).

A futásidő alatt betöltődő (pl. nem az alkalmazáshoz csomagolt) tolmácsolt nyelvet (JavaScript, Python, Lua stb.) tartalmazó alkalmazások vagy harmadik félhez tartozó kódok (pl. SDK-k) nem tehetik lehetővé a Google Play irányelveinek megsértését.

Nem engedélyezünk olyan kódokat, amelyek biztonsági réseket hoznak létre vagy használnak ki. Az alkalmazásbiztonság növelését célzó programunk , további, naprakész tájékoztatást nyújt a

fejlesztőknek jelzett legfrissebb biztonsági problémákról.

Néhány példa a gyakori irányelvsértésekre:

Az eszközzel és hálózattal való visszaélés gyakori példái:

- Olyan alkalmazások, melyek más alkalmazások hirdetésmegjelenítési mechanizmusait akadályozzák vagy módosítják.
- Játékbeli csalást elősegítő alkalmazások, amelyek befolyásolják a játékmenetet más alkalmazásokban.
- Olyan alkalmazások, amelyek elősegítik szolgáltatások, szoftverek vagy hardverek feltörését, vagy megkerülik a biztonsági védelmeket, illetve ezekkel kapcsolatban adnak útmutatást.
- Olyan alkalmazások, amelyek az Általános Szerződési Feltételek megsértésével érnek el vagy használnak valamilyen szolgáltatást vagy API-t.
- Olyan alkalmazások, amelyek nem jogosultak az engedélyezőlistára való felvételre , és megpróbálják megkerülni a rendszer energiakezelését .
- Azok az alkalmazások, amelyek proxyszolgáltatást nyújtanak harmadik feleknek, csak akkor tehetik ezt meg az alkalmazásokban, ha ez az elsődleges, felhasználók számára nyújtott, alapvető rendeltetésük;
- A Google Playen kívüli forrásból futtatható kódot, például .dex fájlokat vagy natív kódot letöltő alkalmazások vagy harmadik félhez tartozó kódok (pl. SDK-k).
- Olyan alkalmazások, amelyek a felhasználó előzetes hozzájárulása nélkül más alkalmazásokat telepítenek az eszközre.
- Olyan alkalmazások, amelyek rosszindulatú programra mutató linket tartalmaznak, vagy elősegítik a rosszindulatú programok terjesztését vagy telepítését.
- Alkalmazások vagy harmadik félhez tartozó kódok (pl. SDK-k), amelyek webes nézetet tartalmaznak hozzáadott interfészinjekciós JavaScripttel, és megbízhatatlan webes tartalmakat (pl. http:// URL-címeket) vagy olyan ellenőrizetlen URL-címeket töltenek be, amelyek megbízhatatlan forrásból származnak (pl. nem megbízható intentek URL-címeiből).
- Olyan alkalmazások, amelyek a teljes képernyős intentengedélyek használatával arra kényszerítik a felhasználókat, hogy tevékenységeket végezzenek zavaró hirdetésekkel vagy értesítésekkel.

Az előtérben futó szolgáltatás használata

Az előtérben futó szolgáltatással kapcsolatos engedély biztosítja a felhasználó számára látható előtérben futó szolgáltatások megfelelő használatát. Az Android 14-es vagy annál magasabb verziót célzó alkalmazások esetében meg kell adnod egy érvényes előtérben futó szolgáltatási típust az alkalmazásodban használt minden egyes előtérben futó szolgáltatáshoz, és deklarálnod kell az adott típusnak megfelelő, előtérben futó szolgáltatási engedélyt. Például ha az alkalmazásod használati esetének szüksége van a térképes földrajzihely-meghatározásra, akkor deklarálnod kell a FOREGROUND_SERVICE_LOCATION engedélyt az alkalmazásod manifestjében.

Az alkalmazások csak akkor deklarálhatnak előtérben futó szolgáltatási engedélyt, ha:

- a használat az alkalmazás alapvető funkciójához kapcsolódó, a felhasználók számára előnyös funkciót biztosít,
- a használatot a felhasználó kezdeményezi, vagy a használat a felhasználó által érzékelhető (például hang egy dal lejátszásakor, médiatartalom átküldése egy másik eszközre, pontos és egyértelmű felhasználói értesítés, felhasználói kérés a fotók felhőbe feltöltésével kapcsolatban),
- a használatot megszüntetheti vagy szüneteltetheti a felhasználó,
- a használatot nem tudja megszakítani vagy késleltetni a rendszer anélkül, hogy az ne okozna negatív felhasználói élményt, vagy ne okozná azt, hogy a felhasználó által elvárt funkció ne az elvárásnak megfelelően működjön (például a telefonhívásnak azonnal el kell indulnia, és nem késleltetheti a rendszer),
- a használat csak a feladat befejezéséhez szükséges ideig tart.

A következő előtérben futó szolgáltatási használati esetek mentesülnek a fenti kritériumok alól:

- systemExempted vagy shortService előtérben futó szolgáltatási típusok;
- csak dataSync előtérben futó szolgáltatási típus Play Asset Delivery funkciók használata esetén.

Az előtérben futó szolgáltatás használatáról bővebb ismertetést itt találsz.

Felhasználó által kezdeményezett adatátviteli munkák

Az alkalmazások csak akkor használhatják a felhasználó által kezdeményezett adatátviteli munkák API-t, ha:

- a használatot a felhasználó kezdeményezte;
- a használat célja hálózati adatátviteli feladatok teljesítése;
- a használat csak az adatátvitel befejezéséhez szükséges ideig tart.

A felhasználó által kezdeményezett adatátviteli API-król bővebb ismertetést itt találsz.

A Flag Secure beállítással kapcsolatos követelmények

A FLAG_SECURE az alkalmazás kódjában deklarált, annak jelzésére szolgáló megjelenítési jelző, hogy az alkalmazás kezelőfelülete olyan érzékeny adatokat tartalmaz, amelyeket az alkalmazás használata közben egy biztonságos felületre célszerű korlátozni. A jelző annak megelőzésére szolgál, hogy az adatok képernyőképen jelenjenek meg vagy pedig hogy nem biztonságos megjelenítőkön tekintsék meg őket. A fejlesztők olyankor deklarálják, amikor az alkalmazás tartalmát nem volna célszerű közvetíteni, megtekinteni vagy máshogy továbbítani az alkalmazáson vagy a felhasználó eszközén kívülre.

Biztonsági és adatvédelmi célokból a Google Playen terjesztett valamennyi alkalmazásnak tiszteletben kell tartania más alkalmazások FLAG_SECURE deklarációját. Ez azt jelenti, hogy az alkalmazások nem könnyíthetik meg a FLAG_SECURE beállítások megkerülését más alkalmazásokban, illetve nem hozhatnak létre erre szolgáló megoldásokat.

A kisegítő eszköznek minősülő alkalmazások mentesülnek e követelmény alól, amennyiben nem továbbítanak, mentenek vagy tárolnak gyorsítótárban a FLAG_SECURE jelző által védett tartalmat a felhasználó eszközén kívüli hozzáférés céljára.

Alkalmazások, amelyek eszközalapú Android-tárolókon futnak

Az eszközalapú Android-tárolóalkalmazások olyan környezeteket biztosítanak, amelyek egy mögöttes Android operációs rendszer egészét vagy részeit szimulálják. A környezetekben tapasztalható élmény nem feltétlenül tükrözi az Android biztonsági funkcióinak teljes csomagját, ezért a fejlesztők dönthetnek úgy, hogy hozzáadnak egy biztonságos környezet manifestjelölőt, így közölhetik az eszközalapú Android-tárolókkal, hogy nem működhetnek a szimulált Android-környezetükben.

Biztonságos környezet manifestjének jelzője

REQUIRE_SECURE_ENV : olyan jelző, amelyet deklarálni lehet az alkalmazás manifestjében, így jelezve, hogy az alkalmazást tilos futtatni eszközalapú Android-tároló alkalmazásokban. Biztonsági és adatvédelmi célokból az eszközalapú Android-tárolókat kínáló alkalmazásoknak tiszteletben kell tartaniuk az összes olyan alkalmazást, amely deklarálja ezt a jelzőt, illetve:

- Ennél a jelölőnél tekintsd át az eszközalapú Android-tárolóba betölteni kívánt alkalmazások manifestjeit.
- Ne történjen meg azon alkalmazások betöltése, amelyek bejelentették ezt a jelölőt az eszközalapú Android-tárolójuknál.
- Ne működjön proxyként API-k hozzáférésénél vagy hívásánál az eszközön, hogy azok telepítettként jelenjenek meg a tárolóban.
- Ne hozzon létre megkerülő megoldásokat a jelölő megkerülésére, és ne segítse ezeket (például egy alkalmazás régebbi verziójának betöltése az aktuális alkalmazás REQUIRE_SECURE_ENV jelölőjének

kikerülése céljából).

További információt találsz erről az irányelvről a Súgóban.

Megtévesztő viselkedés

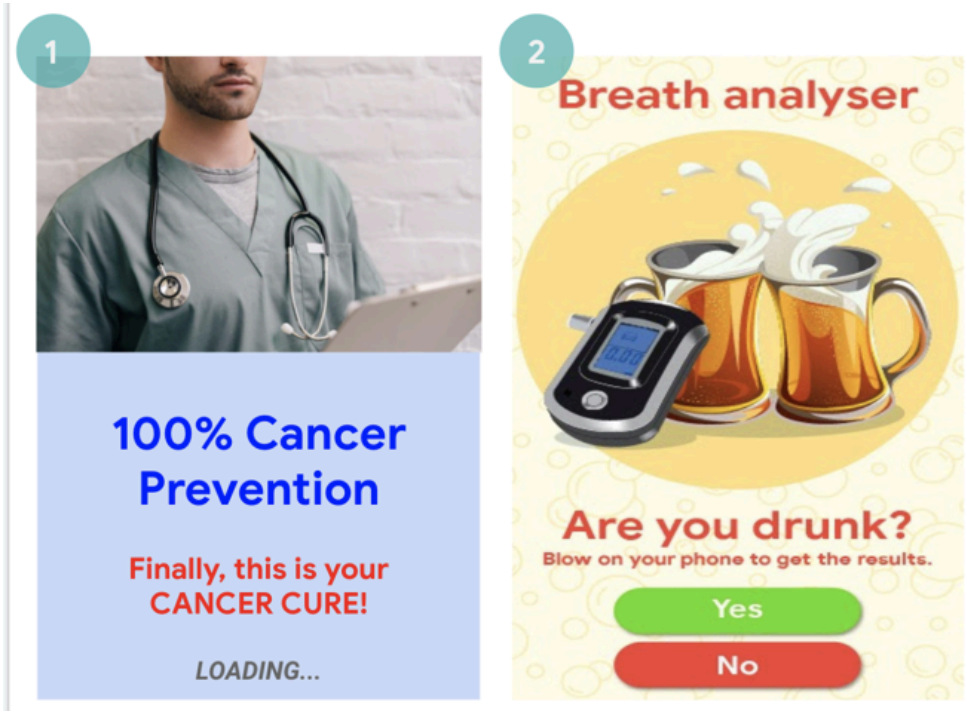
Nem engedélyezünk olyan alkalmazásokat, amelyek megpróbálják félrevezetni a felhasználókat, vagy tisztességtelen magatartást tesznek lehetővé. Ide tartoznak például a lehetetlen funkciót nyújtó alkalmazások. Az alkalmazásoknak pontos nyilatkozatot, leírást és képeket/videót kell biztosítaniuk funkcionalitásukról a metaadatok minden részében. Az alkalmazások nem kísérelhetik meg utánozni az operációs rendszer vagy más alkalmazások funkcióit és figyelmeztetéseit. Az eszköz beállításait csak a felhasználó tudtával és beleegyezésével szabad megváltoztatni, és csak akkor, ha a felhasználó visszavonhatja a változtatást.

Félrevezető állítások

Nem engedélyezzük azokat az alkalmazásokat, amelyek hamis vagy félrevezető információkat vagy állításokat tartalmaznak a leírásban, a címben, az ikonokon vagy a képernyőképeken.

Néhány példa a gyakori irányelvsértésekre:

- A céljukat megtévesztő módon, illetve nem pontosan és egyértelműen leíró alkalmazások:
  - Olyan alkalmazás, amely leírása és képernyőképei alapján versenyzős játék, de valójában logikai játék, amely egy autó képét használja.
  - Olyan alkalmazás, amely vírusirtó alkalmazásként tünteti fel magát, de valójában csak szöveges útmutatót tartalmaz a vírusok eltávolításához.
- Nem megvalósítható funkciókat kínáló alkalmazások (például rovarriasztó alkalmazások), akkor is, ha ugratásként, átverésként, viccként stb. vannak feltüntetve.
- Helytelenül besorolt alkalmazások, beleértve, de nem kizárólagosan az alkalmazás értékelésére és az alkalmazás kategóriájára vonatkozó besorolást.
- Bizonyíthatóan megtévesztő vagy hamis tartalom, amely megzavarhatja a szavazási folyamatokat, illetve a választások eredményéről szól.
- Olyan alkalmazások, amelyek hamisan állítják, hogy kormányzati szervhez tartoznak, vagy amelyek olyan kormányzati szolgáltatásokat biztosítanak vagy segítenek elő, amelyekre nem kaptak kellő felhatalmazást.
- Alkalmazások, amelyek hamisan állítják, hogy valamely ismert szervezet vagy személy hivatalos alkalmazásai. A szükséges engedélyek és jogok nélkül tilos olyan címeket adni, mint például a „Justin Bieber hivatalos alkalmazása”.



(1) Ez az alkalmazás olyan orvosi vagy egészségüggyel kapcsolatos állításokat tartalmaz (rák gyógyítása), amelyek félrevezetők.
(2) Ez az alkalmazás állítása szerint olyan funkciókkal rendelkezik, amelyek megvalósítása lehetetlen (telefon használata alkoholszondaként).

Az eszköz beállításainak megtévesztő módosítása

Nem engedélyezzük azokat az alkalmazásokat, amelyek a felhasználó eszközének beállításait vagy funkcióit az alkalmazáson kívül, a felhasználó tudomása és beleegyezése nélkül módosítják. Az eszközbeállítások és -funkciók közé tartoznak a rendszer- és böngészőbeállítások, a könyvjelzők, a parancsikonok, az ikonok, a modulok, valamint az alkalmazások megjelenítése a kezdőképernyőn.

Ezenkívül nem engedélyezzük a következőket sem:

- Olyan alkalmazásokat, amelyek a felhasználó tudtával, ám nem könnyen visszafordítható módon módosítják az eszköz beállításait vagy funkcióit.
- Olyan alkalmazásokat vagy hirdetéseket, amelyek harmadik fél számára nyújtott szolgáltatásként vagy hirdetési célból módosítják az eszköz beállításait vagy funkcióit.
- Olyan alkalmazásokat, amelyek félrevezető módon ráveszik a felhasználókat, hogy távolítsák el vagy tiltsák le harmadik felek alkalmazásait, illetve módosítsák az eszköz beállításait vagy funkcióit.
- Olyan alkalmazásokat, amelyek arra bátorítják vagy ösztönzik a felhasználókat, hogy távolítsák el vagy tiltsák le harmadik felek alkalmazásait, illetve módosítsák az eszköz beállításait vagy funkcióit – kivéve, ha ez egy igazoltan biztonsági funkciókat ellátó szolgáltatás része.

Tisztességtelen magatartás támogatása

Nem engedélyezünk olyan alkalmazásokat, amelyek segítségével a felhasználók félrevezethetnek másokat, vagy amelyek funkciói bármilyen tekintetben megtévesztők. Ilyenek lehetnek többek között a személyazonosító igazolványokat, társadalombiztosítási számokat, útleveleket, diplomákat, hitelkártyákat, bankszámlákat és jogosítványokat létrehozó vagy azok létrehozását segítő alkalmazások. Az alkalmazásoknak pontos nyilatkozatokat, címeket, leírásokat és képeket/videót kell biztosítaniuk funkcióikról és/vagy tartalmaikról, továbbá olyan módon kell működniük, ahogyan a felhasználók észszerűen és pontosan elvárhatják.

További alkalmazásforrások (például játékelemek) csak akkor tölthetők le, ha az alkalmazás használatához nélkülözhetetlenek. A letöltött erőforrásoknak is meg kell felelniük a Google Play

minden irányelvének, és a letöltés megkezdése előtt az alkalmazásnak jóváhagyást kell kérnie a felhasználótól úgy, hogy közli vele a letöltés méretét is.

Az alkalmazások akkor sem mentesülnek irányelveink betartása alól, ha a fejlesztők csak „viccnek szánták” vagy „szórakoztatási célra készítették” őket (és hasonlók).

Néhány példa a gyakori irányelvsértésekre:

- Olyan alkalmazások, amelyek más alkalmazások vagy webhelyek utánzásával ráveszik a felhasználót, hogy személyes vagy hitelesítési adatokat adjon meg.
- Olyan alkalmazások, amelyek beleegyezésüket nem adó személyek vagy jogi személyek ellenőrizetlen vagy valódi telefonszámait, kapcsolatfelvételi adatait, címeit és személyazonosításra alkalmas adatait tartalmazzák vagy jelenítik meg.
- Olyan alkalmazások, amelyek eltérő alapfunkciókkal rendelkeznek a felhasználó földrajzi helyzete, az eszközparaméterek vagy egyéb, felhasználóalapú adatok alapján, amennyiben ezek a különbségek nincsenek jól látható módon feltüntetve a felhasználó számára az áruházi adatlapon.
- Olyan alkalmazások, amelyek frissítések útján jelentős mértékben megváltoznak, de az áruházi adatlap nem változik ennek megfelelően, és a felhasználók sem kaptak tájékoztatást a változásról (például az „újdonságok” szakaszban).
- Olyan alkalmazások, melyek a Google Play általi felülvizsgálat során megkísérlik működésük módosítását vagy elrejtését.
- Tartalomelosztó hálózaton (CDN-en) keresztül letöltést indító alkalmazások, amelyek letöltés előtt nem kérik a felhasználó jóváhagyását, és nem adnak tájékoztatást a letöltés méretéről.

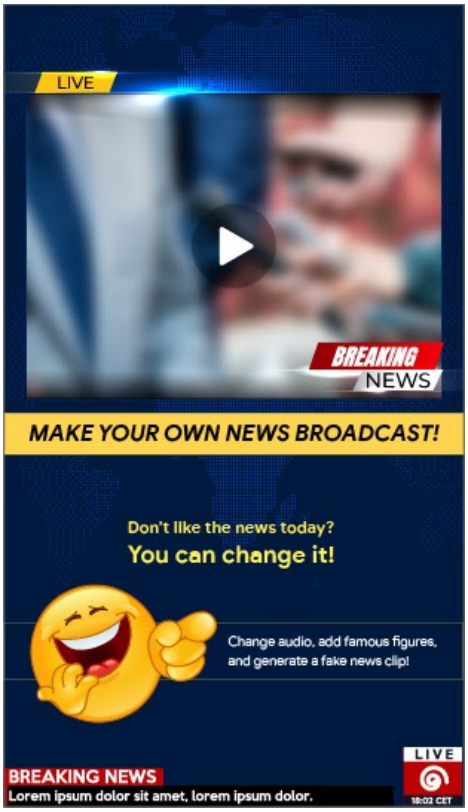
Manipulált médiatartalmak

Nem engedélyezünk olyan alkalmazásokat, amelyek akár audió, akár (mozgó)képi, akár szöveges formában téves vagy félrevezető információk, állítások népszerűsítését vagy létrehozását segítik. Nem engedélyezünk olyan alkalmazásokat, amelyeknek célja bizonyíthatóan félrevezető vagy megtévesztő, kényes eseménnyel, politikával, társadalmi problémával vagy más közérdekű üggyel kapcsolatban esetleg ártalmas képek, videók vagy szövegek népszerűsítse vagy terjesztése.

Egyértelmű tájékoztatást kell nyújtania, vagy vízjelet kell alkalmaznia minden olyan alkalmazásnak, amely a szokványos vagy sajtóban elfogadható mértéken túlmenően manipulál vagy módosít médiatartalmakat úgy, hogy a változtatás nem feltétlenül nyilvánvaló az átlagos felhasználó számára. Kivételt tehetünk a közérdeket szolgáló vagy egyértelműen szatírának, paródiának minősülő esetekben.

Néhány példa a gyakori irányelvsértésekre:

- Olyan alkalmazások, amelyek közismert személyt helyeznek el politikailag kényes esemény során zajló demonstrációt ábrázoló képen/videón.
- Olyan alkalmazások, amelyek kényes eseményen részt vevő közismert személyt vagy sajtóforrást használnak fel saját tartalommanipulációs képességeik hirdetésére az áruházi adatlapon.
- Olyan alkalmazások, amelyek videófelvételek manipulálásával híradót utánoznak.



(1) Ez az alkalmazás lehetővé teszi videófelvételek vízjel nélküli manipulálását híradó utánzása és híres személyek vagy közszereplők elhelyezése céljából.

Viselkedés átláthatósága

Az alkalmazásod működésének – észszerű határok között – egyértelműnek kell lennie a felhasználók számára; az alkalmazásod ne tartalmazzon rejtett, használaton kívüli vagy nem dokumentált funkciókat. Az alkalmazás-felülvizsgálatok kijátszására szolgáló technikák nem engedélyezettek. Előfordulhat, hogy az alkalmazásoknak további részleteket kell megadniuk a felhasználói biztonság, a rendszerintegritás és az irányelveknek való megfelelés biztosítása érdekében.

Megtévesztés

Nem engedélyezünk olyan alkalmazásokat és fejlesztői fiókokat, amelyek:

- más személy vagy szervezet adataival élnek vissza, vagy amelyek eltitkolják elsődleges céljukat és tulajdonosuk kilétét, vagy megtévesztő információt adnak meg róluk;
- a felhasználók félrevezetésére irányuló szervezett tevékenységet folytatnak. Ide tartoznak többek között azok az alkalmazások és fejlesztői fiókok, amelyek eltitkolják származási országukat, vagy megtévesztő információt adnak meg róla, vagy tartalmaikkal más országok felhasználóit célozzák meg;
- más alkalmazásokkal, webhelyekkel, fejlesztőkkel vagy egyéb fiókokkal összehangolva elrejtik a fejlesztő vagy az alkalmazás azonosítóját és más fontos adatokat, vagy félrevezető információkat közölnek róluk, amikor az alkalmazás tartalmai politikával, társadalmi problémákkal, valamint közügyekkel kapcsolatosak.

A Google Play megcélzott API-szintre vonatkozó irányelve

Annak érdekében, hogy a felhasználóknak biztonságos élményben legyen részük, a Google Play a következő megcélzott API-szinteket várja el **minden alkalmazástól**:

Az új alkalmazásoknak és alkalmazásfrissítéseknek KÖTELEZŐ megcélozniuk egy Android API-szintet a legutóbbi fő Android operációs rendszer verziójának kiadásától számított egy éven belül. A követelménynek meg nem felelő új alkalmazások és alkalmazásfrissítések beküldését nem engedélyezzük a Play Console-on.

Meglévő, de még nem frissített Google Play alkalmazások és olyanok, amelyek nem céloznak meg egy API-szintet a legutóbbi fő Android-kiadástól számított két éven belül, nem lesznek elérhetők az Android operációs rendszer újabb verzióit futtató eszközökkel rendelkező új felhasználók számára. Azok a felhasználók, akik korábban már telepítették az alkalmazást a Google Play Áruházból, továbbra is felfedezhetik, újratelepíthetik és használhatják az alkalmazást az általa támogatott bármely Android operációs rendszeren.

Ha technikai tanácsra van szükséged azzal kapcsolatban, hogy miként felelhetsz meg a megcélzott API-szinttel kapcsolatos követelménynek, tekintsd meg az áttelepítési útmutatót .

A pontos idővonalat és a kivételeket ez a súgócikk tartalmazza.

SDK-követelmények

Az alkalmazásfejlesztők gyakran harmadik félhez tartozó kódot (például egy SDK-t) használnak alkalmazásaik alapvető funkcióinak és szolgáltatásainak integrálásához. Amikor egy SDK-t integrálsz az alkalmazásodba, figyelned kell arra, hogy meg tudd őrizni felhasználóid biztonságát, és elkerüld alkalmazásod sebezhetőségét. Ebben a szakaszban bemutatunk néhány SDK-kkal kapcsolatos adatvédelmi és biztonsági követelményt, amelyek segítségével a fejlesztők biztonságosan integrálhatnak SDK-kat alkalmazásaikba.

Ha alkalmazásod SDK-t tartalmaz, a te felelősséged annak biztosítása, hogy a harmadik fél kódja és gyakorlatai miatt az alkalmazásod ne sértse meg a Google Play Fejlesztői Programszabályzatát. Fontos tisztában lenni azzal, hogy az alkalmazásaidban található SDK-k miként kezelik a felhasználói adatokat, továbbá tisztában kell lenned azzal is, hogy ezek az SDK-k milyen engedélyeket használnak, milyen adatokat gyűjtenek, és miért gyűjtik ezeket az adatokat. Ne feledd, az SDK-k adatgyűjtési és -kezelési gyakorlatának meg kell felelnie alkalmazásod irányelv szerinti adathasználati gyakorlatának.

Annak érdekében, hogy az általad használt SDK ne sértse meg az irányelvi követelményeket, részletesen olvasd el és értelmezd a következő irányelveket, és vedd figyelembe az SDK-kra vonatkozó meglévő követelményeiket:

Felhasználói adatokra vonatkozó irányelvek

A fejlesztőnek a felhasználói adatokat (például a felhasználóktól vagy a felhasználókról gyűjtött adatokat, beleértve az eszközadatokat is) átlátható módon kell kezelnie. Ez azt jelenti, hogy nyilvánosságra kell hozni a felhasználói adatok hozzáférését, gyűjtését, felhasználását, kezelését és megosztását az alkalmazásból, és az adatok felhasználását a nyilvánosságra hozott irányelveknek megfelelő célokra kell korlátozni.

Ha harmadik féltől származó kódot (például SDK-t) szerepeltetsz az alkalmazásodban, akkor biztosítanod kell, hogy az alkalmazásodban használt, harmadik fél által biztosított kód, valamint az alkalmazásodból származó adatok harmadik fél általi feldolgozására irányuló gyakorlatok megfeleljenek a Google Play Fejlesztői Programszabályzatnak, amely a felhasználásra és a közzétételre vonatkozó előírásokat is tartalmaz. Biztosítanod kell például, hogy az SDK-szolgáltatók ne adjanak el személyes és érzékeny felhasználói adatokat az alkalmazásból. Ez a követelmény attól függetlenül érvényes, hogy a felhasználói adatok továbbítása a szerverre történő elküldés után vagy harmadik fél kódjának az alkalmazásba történő beágyazásával történik.

Személyes és bizalmas felhasználói adatok

- Az alkalmazásban megszerzett személyes és bizalmas felhasználói adatokhoz való hozzáférést, valamint ezek gyűjtését, felhasználását és megosztását az alkalmazásra és a szolgáltatás funkcióira és az irányelvekben feltüntetett célokra kell korlátozni a felhasználó által észszerűen elvárható módon:

- A személyes és bizalmas felhasználói adatokhoz hozzáférést kibővítő alkalmazásoknak be kell tartaniuk a Google Play hirdetési irányelveit.
- Minden személyes és bizalmas felhasználói adatot biztonságosan kell kezelni, amibe beletartozik az is, hogy az adattovábbítás valamilyen modern titkosítással (például HTTPS-protokollal) történjen.
- Az Android-engedélyek által korlátozott adatokhoz való hozzáférés előtt futásidőben küldhető engedélykérést kell alkalmazni (ha lehetséges).

Személyes és bizalmas felhasználói adatok értékesítése

Ne értékesíts személyes és bizalmas felhasználói adatokat.

- Az „értékesítés” személyes és érzékeny felhasználói adatok cseréjét vagy átadását jelenti harmadik félnek pénzbeli ellenérték fejében.
  - A személyes és érzékeny felhasználói adatok felhasználó által kezdeményezett továbbítása (például amikor a felhasználó az alkalmazás egy funkcióját használja arra, hogy fájlt továbbítson egy harmadik félnek, vagy amikor a felhasználó úgy dönt, hogy egy kifejezetten kutatási célú alkalmazást használ) nem minősül értékesítésnek.

A jól látható közlésre és a hozzájárulásra vonatkozó követelmények

Azokban az esetekben, amikor a személyes és érzékeny felhasználói adatok hozzáférése, gyűjtése, felhasználása vagy megosztása az alkalmazásban nem felel meg az adott termék vagy funkció felhasználója észszerű elvárásainak, meg kell felelned a felhasználói adatokra vonatkozó irányelvek jól látható közlésre és hozzájárulásra vonatkozó követelményeinek.

Ha alkalmazásodban olyan, harmadik féltől származó kód (például SDK) szerepel, amelynek célja alapértelmezés szerint a személyes és érzékeny felhasználói adatok gyűjtése, akkor a Google Playtől érkezett kéréstől számított 2 héten belül (vagy ha a Play kérésében ennél hosszabb határidő szerepel, akkor az adott időn belül) megfelelő bizonyítékot kell benyújtanod arra vonatkozóan, hogy az alkalmazásod megfelel az irányelvben szereplő, a jól látható közlésre és a hozzájárulásra vonatkozó követelményeknek, köztük a harmadik fél kódjának segítségével az adatokhoz való hozzáférésre, az adatgyűjtésre, adathasználatra és adatmegosztásra érvényes követelményeknek is.

Ne felejts el meggyőződni arról, hogy az alkalmazásod által használt harmadik félhez tartozó kód (például egy SDK) nem sérti meg a felhasználói adatokra vonatkozó irányelveket.

Ha további információra van szükséged a jól látható közlésre és a hozzájárulásra vonatkozó követelményekről, tekintsd meg ezt a Súgócikket.

Példák SDK által okozott irányelvsértésekre

- Olyan SDK-val rendelkező alkalmazás, amely személyes és érzékeny felhasználói adatokat gyűjt, és ezeket az adatokat nem kezeli úgy, mint amelyek a jelen felhasználói adatokra vonatkozó irányelvek, a hozzáférésnek, az adatkezelésnek (beleértve a tiltott értékesítést), valamint a feltűnő közzétételi és hozzájárulási követelményeknek a hatálya alá tartoznak.
- Olyan SDK-t integráló alkalmazás, amely alapértelmezés szerint személyes és bizalmas adatokat gyűjt, és ezzel megsérti a felhasználói hozzájárulásra és a jól látható nyilatkozatra vonatkozó irányelvi követelményeket.
- Olyan SDK-val rendelkező alkalmazás, amely állítása szerint kizárólag csalás és visszaélés megelőzése céljából gyűjt személyes és bizalmas adatokat, azonban az SDK a gyűjtött adatokat hirdetési vagy elemzési célból harmadik felekkel is megosztja.
- Olyan SDK-val rendelkező alkalmazás, amely továbbítja a felhasználók telepített csomagjaira vonatkozó információkat, azonban nem felel meg a jól látható nyilatkozatra vonatkozó iránymutatásoknak és/vagy az adatvédelmi irányelvekre vonatkozó iránymutatásoknak.
  - Tanulmányozd a nemkívánatos mobilszoftverekre vonatkozó irányelvet is.

A személyes és bizalmas adatokhoz való hozzáférés további követelményei

Az alábbi táblázat ismerteti a konkrét tevékenységekre vonatkozó követelményeket.

Tevékenység	Követelmény
Az alkalmazás állandó eszközazonosítókat (pl. IMEI, IMSI, SIM-sorozatszám stb.) gyűjt vagy kapcsol össze más adatokkal	Az állandó eszközazonosítók nem kapcsolhatók össze más személyes és bizalmas felhasználói adatokkal vagy visszaállítható eszközazonosítókkal, a következők kivételével:

	• SIM-alapú azonosításhoz kötődő telefonos szolgáltatások (pl. szolgáltatói fiókkal összekapcsolt Wi-Fi-hívás); • eszköztulajdonosi módot használó vállalati eszközkezelő alkalmazások. Ezeket a felhasználási módokat egyértelműen a felhasználók tudomására kell hozni a felhasználói adatokra vonatkozó irányelveknek megfelelően. Ez a segédanyag bemutatja az egyéb használható egyedi azonosítókat. Az androidos hirdetésazonosítókkal kapcsolatos további útmutatás a hirdetési irányelvekben található.
Az alkalmazás célközönsége gyermekeket foglal magában	Alkalmazásod csak olyan SDK-kat tartalmazhat, amelyek öntanúsítással jelezték, hogy használhatók gyermekeknek készült szolgáltatásokban. Az irányelv teljes szövege és a követelmények itt találhatók: Családbarát öntanúsító hirdetési SDK program.

Példák SDK által okozott irányelvsértésekre

- Olyan SDK-t használó alkalmazás, amely összeköti az Android-azonosítót a tartózkodási hellyel
- Olyan SDK-t használó alkalmazás, amely hirdetési vagy elemzési célból összekapcsolja az állandó eszközazonosítókat és az AAID-t.
- Olyan SDK-t használó alkalmazás, amely hirdetési célból összekapcsolja az AAID-t és az e-mail-címet.

Adatbiztonsági szakasz

Minden fejlesztőnek egyértelmű és pontos Adatbiztonsági szakaszt kell kitöltenie az összes alkalmazásnál a felhasználói adatok begyűjtésére, felhasználására és megosztására vonatkozóan. Idetartoznak az alkalmazásaikban használt, harmadik féltől származó függvénytárakon vagy SDK-kon keresztül gyűjtött és kezelt adatok is. A fejlesztő felelős a címke tartalmának pontosságáért, és hogy az információk naprakészek legyenek. Adott esetben az Adatbiztonsági szakasznak konzisztensnek kell lennie az alkalmazás adatvédelmi irányelveiben foglaltakkal.

Ebben a súgócikkben további információt találsz az Adatbiztonság szakasz kitöltésével kapcsolatban.

Itt találod a felhasználói adatokra vonatkozó irányelveket.

Engedélyek és bizalmas információhoz hozzáférő API-k irányelve

Az engedély- és a bizalmas információkhoz hozzáférő API-kéréseket közérthető módon kell megfogalmazni a felhasználó számára. Csak olyan engedélyeket és bizalmas információkhoz hozzáférő API-kat kérhetsz, amelyek az alkalmazás meglévő, Google Play-adatlapján ismertetett funkcióinak vagy szolgáltatásainak megvalósításához szükségesek. Nem használhatsz sem olyan engedélyeket, sem olyan bizalmas információkhoz hozzáférő API-kat, amelyek nem nyilvános, megvalósításra nem kerülő vagy nem engedélyezett funkciókhoz vagy célokra biztosítanak hozzáférést a felhasználói vagy eszközadatokhoz. Az engedélyeknek vagy a bizalmas információkhoz hozzáférő API-knak köszönhetően megismert személyes vagy bizalmas adatok értékesítése, illetve értékesítési célból történő megosztása tilos.

Itt találod az Engedélyek és bizalmas információhoz hozzáférő API-k irányelvét.

Példák SDK által okozott irányelvsértésekre

- Alkalmazásod olyan SDK-t tartalmaz, amely nem engedélyezett vagy nem közölt célból kéri a helyadatok használatát a háttérben.
- Alkalmazásod olyan SDK-t tartalmaz, amely továbbítja a read_phone_state Android-engedélyből a felhasználó beleegyezése nélkül kinyert IMEI-t.

Rosszindulatú programokra vonatkozó irányelv

Rosszindulatú programokra vonatkozó irányelvünk egyszerű: az Android ökoszisztémája – a Google Play Áruházzal együtt – és a felhasználók eszközei legyenek mentesek mindennemű kártékony viselkedéstől (azaz rosszindulatú programtól). Ezzel az alapelvvel arra törekszünk, hogy biztonságos Android-ökoszisztémát nyújthassunk felhasználóinknak és androidos eszközeiknek.

Rosszindulatú programnak tekintendő minden olyan kód, amely veszélynek teszi ki a felhasználót, a felhasználó adatait vagy a felhasználó eszközét. A rosszindulatú programok közé tartoznak (többek között) az olyan potenciálisan kártékony alkalmazások, futtatható állományok és keretrendszer-módosítások, melyek például trójai kártevőket, adathalász kísérleteket és kémprogramokat rejtenek. A rosszindulatú programok kategóriáit folyamatosan bővítjük.

A jelen irányelv követelményei bármely harmadik féltől származó kódra (például SDK-ra) vonatkoznak, amelyet az alkalmazásodba beépítesz.

Tekintsd meg a Rosszindulatú programokra vonatkozó irányelvet.

Példák SDK által okozott irányelvsértésekre

- olyan alkalmazás, amely rosszindulatú szoftvereket terjesztő szolgáltatók SDK-könyvtárait tartalmazza;
- olyan alkalmazások, amelyek áthágják az Android engedélykezelő rendszerét, vagy hitelesítési adatokat (pl. OAuth-tokeneket) szereznek más alkalmazásoktól;
- olyan alkalmazások, amelyek saját eltávolításuk vagy leállításuk megakadályozása érdekében visszaélnek bizonyos funkciókkal;
- olyan alkalmazások, amelyek letiltják a SELinux modult;
- olyan SDK-t tartalmazó alkalmazás, amely megsérti az Android engedélykezelő rendszerét úgy, hogy magasabb szintű jogosultságokat szerez az eszközadatokhoz való hozzáféréshez, mindezt nem közölt célból;
- olyan SDK-t tartalmazó alkalmazás, amely kódja megtéveszti a felhasználókat, hogy azok a mobilszámlájuk terhére előfizessenek bizonyos tartalmakra vagy megvásárolják azokat.

SDK-k használata alkalmazásokban

Ha alkalmazásod SDK-t tartalmaz, a te felelősséged annak biztosítása, hogy a harmadik fél kódja és gyakorlatai miatt az alkalmazásod ne sértse meg a Google Play Fejlesztői Programszabályzatát. Fontos tisztában lenni azzal, hogy az alkalmazásaidban található SDK-k miként kezelik a felhasználói adatokat, továbbá tisztában kell lenned azzal is, hogy ezek az SDK-k milyen engedélyeket használnak, milyen adatokat gyűjtenek, és miért gyűjtik ezeket az adatokat.

SDK-követelmények

Az alkalmazásfejlesztők gyakran harmadik félhez tartozó kódot (például egy SDK-t) használnak alkalmazásaik alapvető funkcióinak és szolgáltatásainak integrálásához. Amikor egy SDK-t integrálsz az alkalmazásodba, figyelned kell arra, hogy meg tudd őrizni felhasználóid biztonságát, és elkerüld alkalmazásod sebezhetőségét. Ebben a szakaszban bemutatunk néhány SDK-kkal kapcsolatos adatvédelmi és biztonsági követelményt, amelyek segítségével a fejlesztők biztonságosan integrálhatnak SDK-kat alkalmazásaikba.

Ha alkalmazásod SDK-t tartalmaz, a te felelősséged annak biztosítása, hogy a harmadik fél kódja és gyakorlatai miatt az alkalmazásod ne sértse meg a Google Play Fejlesztői Programszabályzatát. Fontos tisztában lenni azzal, hogy az alkalmazásaidban található SDK-k miként kezelik a felhasználói adatokat, továbbá tisztában kell lenned azzal is, hogy ezek az SDK-k milyen engedélyeket használnak, milyen adatokat gyűjtenek, és miért gyűjtik ezeket az adatokat. Ne feledd, az SDK-k adatgyűjtési és -kezelési gyakorlatának meg kell felelnie alkalmazásod irányelv szerinti adathasználati gyakorlatának.

Annak érdekében, hogy az általad használt SDK ne sértse meg az irányelvi követelményeket, részletesen olvasd el és értelmezd a következő irányelveket, és vedd figyelembe az SDK-kra vonatkozó meglévő követelményeiket:

A magasabb szintű hozzáférést szerző alkalmazásokat, amelyek a felhasználó engedélye nélkül rootolják az eszközt, rootoló alkalmazásoknak nevezzük.

Kémprogram

A kémprogram olyan rosszindulatú alkalmazás, kód vagy viselkedés, amely olyan felhasználói vagy eszközadatokat gyűjt, juttat ki vagy oszt meg, amelyek nem a házirendnek megfelelő funkciókhoz kapcsolódnak.

Kémprogramnak minősül az a rosszindulatú kód vagy viselkedés is, amellyel kapcsolatban fontolóra vehető, hogy a felhasználó után kémkedik, vagy pedig megfelelő értesítés vagy beleegyezés nélkül juttat ki adatokat.

Tekintsd meg a kémprogramokra vonatkozó teljes irányelvet.

SDK-okozta kémprogrammal történő irányelvsértés többek között például a következő:

- Olyan alkalmazás, amely olyan SDK-t használ, amely hang- vagy hívásfelvételekből továbbít adatokat, ha az nem kapcsolódik az irányelveknek megfelelő alkalmazásfunkciókhoz.
- A rosszindulatú, harmadik féltől származó kódot (például SDK-t) tartalmazó alkalmazás, amely a felhasználó számára váratlan módon és/vagy a felhasználó megfelelő értesítése vagy beleegyezése nélkül továbbít adatot az eszközről.

Nemkívánatos mobilszoftverekre vonatkozó irányelv

Átlátható viselkedés és egyértelmű tájékoztatás

Minden kódnak teljesítenie kell a felhasználóknak tett ígéreteket. Az alkalmazásoknak minden bemutatott funkciót biztosítaniuk kell. Az alkalmazásoknak nem szabad összezavarniuk a felhasználókat.

Néhány irányelvsértés:

- Hirdetési csalás
- Bizalomra épülő manipuláció

A felhasználói adatok védelme

A személyes és bizalmas felhasználói adatokhoz való hozzáférésnek, valamint az ilyen adatok használatának, gyűjtésének és megosztásának egyértelműnek és átláthatónak kell lennie. A felhasználói adatok felhasználása során az összes vonatkozó felhasználóiadat-irányelvet követni kell, és meg kell tenni minden óvintézkedést az adatok védelme érdekében.

Néhány irányelvsértés:

- Adatgyűjtés (vö. kémprogram)
- Korlátozott engedélyekkel való visszaélés

Tekintsd meg a teljes Nemkívánatos mobilszoftverekre vonatkozó irányelvet

Eszközzel és hálózattal való visszaélésről szóló irányelv

Nem engedélyezünk olyan alkalmazásokat, amelyek jogosulatlan módon zavarják, akadályozzák, károsítják vagy érik el a felhasználó eszközét, illetve más eszközöket, számítógépeket, szervereket, hálózatokat, alkalmazásprogramozási felületeket (API-kat) vagy szolgáltatásokat – köztük az eszközön megtalálható egyéb alkalmazásokat, a Google szolgáltatásait és a mobilszolgáltatói hálózatokat.

Olyan alkalmazások vagy harmadik félhez tartozó kódok (pl. SDK-k), amelyek tolmácsolt nyelvvel rendelkeznek (JavaScript, Python, Lua stb.), és a futásidő alatt töltődnek be (pl. nem részei az alkalmazásnak), nem engedélyezhetik a Google Play irányelveinek megsértését.

Nem engedélyezünk olyan kódokat, amelyek biztonsági réseket hoznak létre vagy használnak ki. Tekintsd át az Alkalmazások biztonságának javítására szolgáló programunkat, amelyből értesülhetsz a fejlesztőknek jelzett legfrissebb biztonsági problémákról.

Tekintsd meg a teljes Eszközzel és hálózattal való visszaélésről szóló irányelvet.

Példák SDK által okozott irányelvsértésekre

- Azok az alkalmazások, amelyek proxyszolgáltatást nyújtanak harmadik feleknek, csak akkor tehetik ezt meg az alkalmazásokban, ha ez az elsődleges, felhasználók számára nyújtott, alapvető rendeltetésük;
- alkalmazásod olyan SDK-t tartalmaz, amely a Google Playtől eltérő forrásból tölt le futtatható kódot (például dex fájlokat vagy natív kódot);
- alkalmazásod olyan SDK-t használ, amely webes nézetet tartalmaz hozzáadott interfészinjekciós JavaScripttel, amely megbízhatatlan webes tartalmakat (pl. http:// URL-címeket) vagy megbízhatatlan forrásokból származó, ellenőrizetlen URL-címeket tölt be (pl. nem megbízható intentek URL-címeiből);
- alkalmazásod olyan SDK-t tartalmaz, amelyben a saját APK-ja frissítésére használatos kód található;
- alkalmazásod olyan SDK-t tartalmaz, amely biztonsági résnek teszi ki a felhasználókat azzal, hogy nem biztonságos kapcsolaton keresztül tölt le fájlokat;
- alkalmazásod olyan SDK-t használ, amely olyan kódot tartalmaz, amely a Google Playen kívüli, Ismeretlen forrásokból származó alkalmazásokat tölt le vagy telepít;
- alkalmazásod olyan SDK-t tartalmaz, amely megfelelő használati eset nélkül használ előtérben futó szolgáltatásokat;
- alkalmazásod olyan SDK-t tartalmaz, amely az irányelvi megfelelőség érdekében használ előtérben futó szolgáltatásokat, de ez az alkalmazásod manifestjében nincs deklarálva.

Megtévesztő viselkedésre vonatkozó irányelv

Nem engedélyezünk olyan alkalmazásokat, amelyek megpróbálják félrevezetni a felhasználókat, vagy tisztességtelen magatartást tesznek lehetővé. Ide tartoznak például a lehetetlen funkciót nyújtó alkalmazások. Az alkalmazásoknak pontos nyilatkozatot, leírást és képeket/videót kell biztosítaniuk funkcionalitásukról a metaadatok minden részében. Az alkalmazások nem kísérelhetik meg utánozni az operációs rendszer vagy más alkalmazások funkcióit és figyelmeztetéseit. Az eszköz beállításait csak a felhasználó tudtával és beleegyezésével szabad megváltoztatni, és csak akkor, ha a felhasználó visszavonhatja a változtatást.

Tekintsd meg a teljes megtévesztő viselkedésre vonatkozó irányelvet

Viselkedés átláthatósága

Az alkalmazásod működésének – észszerű határok között – egyértelműnek kell lennie a felhasználók számára; az alkalmazásod ne tartalmazzon rejtett, használaton kívüli vagy nem dokumentált funkciókat. Az alkalmazás-felülvizsgálatok kijátszására szolgáló technikák nem engedélyezettek. Előfordulhat, hogy az alkalmazásoknak további részleteket kell megadniuk a felhasználói biztonság, a rendszerintegritás és az irányelveknek való megfelelés biztosítása érdekében.

Példa SDK által okozott irányelvsértésre

- Az alkalmazásod olyan SDK-t tartalmaz, amely technikákat használ az alkalmazás-felülvizsgálatok elkerülése érdekében.

Mely Google Play fejlesztői irányelvek kapcsolódnak gyakran az SDK-k által okozott irányelvsértésekhez?

Segítünk gondoskodni róla, hogy az alkalmazásod által használt minden harmadik féltől származó kód megfeleljen a Google Play Fejlesztői programszabályzatának – figyelmesen olvasd el a következő irányelveket:

- Felhasználói adatokra vonatkozó irányelvek
- Engedélyek és bizalmas információhoz hozzáférő API-k
- Eszközzel és hálózattal való visszaéléssel kapcsolatos irányelv
- Rosszindulatú programok
- Nemkívánatos mobilszoftverek
- Családbarát öntanúsító hirdetési SDK program
- Hirdetési irányelvek
- Megtévesztő viselkedés
- Google Play Fejlesztői Programszabályzat

Habár ezek a leggyakrabban érintett irányelvek, fontos megjegyezni, hogy a hibás SDK-kód más, a fentiekben meg nem nevezett irányelveket is megsérthet. Tanulmányozd az összes irányelvet, és maradj naprakész, mivel alkalmazásfejlesztőként a te felelősséged annak biztosítása, hogy az SDK-id az irányelveket betartva kezeljék az alkalmazásadataidat.

További információért keresd fel a Súgót.

Rosszindulatú program

Rosszindulatú programokra vonatkozó irányelvünk egyszerű: az Android ökoszisztémája – a Google Play Áruházzal együtt – és a felhasználók eszközei legyenek mentesek mindennemű kártékony viselkedéstől (azaz rosszindulatú programtól). Ezzel az alapelvvel arra törekszünk, hogy biztonságos Android-ökoszisztémát nyújthassunk felhasználóinknak és androidos eszközeiknek.

Rosszindulatú programnak tekintendő minden olyan kód, amely veszélynek teszi ki a felhasználót, a felhasználó adatait vagy a felhasználó eszközét. A rosszindulatú programok közé tartoznak (többek között) az olyan potenciálisan kártékony alkalmazások, futtatható állományok és keretrendszer-módosítások, melyek például trójai kártevőket, adathalász kísérleteket és kémprogramokat rejtenek. A rosszindulatú programok kategóriáit folyamatosan bővítjük.

A jelen irányelv követelményei bármely harmadik féltől származó kódra (például SDK-ra) vonatkoznak, amelyet az alkalmazásodba beépítesz.

A rosszindulatú programok típusuk és képességeik szerint sokfélék lehetnek, de céljaik általában a következők valamelyike:

- A felhasználói eszköz integritásának károsítása.
- A felhasználó eszköze feletti irányítás megszerzése.
- Olyan, távolról irányított műveletek végrehajtásának lehetővé tétele, amelyekkel a támadó hozzáférést kaphat a fertőzött eszközhöz, majd az eszközt irányíthatja, vagy más módon kihasználhatja.
- Személyes vagy hitelesítési adatok továbbítása az eszközről megfelelő tájékoztatás nyújtása és beleegyezés kérése nélkül.
- Spam vagy parancsok terjesztése a fertőzött eszközről más eszközökre vagy hálózatokra.
- A felhasználó megtévesztése és megkárosítása.

Az alkalmazások, futtatható állományok és keretrendszer-módosítások potenciálisan kártékonyak lehetnek – azaz rosszindulatú viselkedést tanúsíthatnak – még akkor is, ha nem rosszindulatú céllal készültek. Ennek oka, hogy az alkalmazások, a futtatható állományok és a keretrendszer-módosítások számos tényezőtől függően sokféle módon működhetnek. Tehát ami az egyik Android-eszközön kártékony, a másikon teljesen ártalmatlan lehet. Például az Android legújabb verzióját futtató eszközökre nem jelentenek veszélyt azok az alkalmazások, amelyek elavult API-k használata miatt

kártékony viselkedésre vehetők rá, de a sokkal régebbi Androidot futtató eszközök veszélyben lehetnek. Az alkalmazásokat, a futtatható állományokat és a keretrendszer-módosításokat rosszindulatú programként vagy potenciálisan kártékony alkalmazásként (PHA) jelöljük, ha egyértelműen veszélyt jelentenek az Android-eszközöknek és a felhasználóknak akár csak egy kis részére is.

Lentebb különböző típusú rosszindulatú programokat mutatunk be. Ezt két fő okból tesszük: egyrészt azért, mert meggyőződésünk, hogy a felhasználóknak érdemes tisztában lenniük azzal, hogy eszközeiket miként használhatják ki az esetleges támadók, másrészt pedig azért, hogy ezzel is támogassuk az átfogó innovációt és megbízható felhasználói élményt nyújtó, biztonságos ökoszisztéma kialakulását.

További információt a Google Play Protect webhelyén találsz.

Hátsó ajtó

Olyan kód, amely kéretlen, potenciálisan kártékony vagy távolról irányított műveletek végrehajtását teszi lehetővé az eszközön.

Azok a műveletek is ide tartozhatnak, amelyek az alkalmazást, a futtatható állományt vagy a keretrendszer-módosítást a rosszindulatú programok más kategóriájába sorolnák, ha végrehajtásuk automatikus lenne. A hátsó ajtó kifejezés általában arra vonatkozik, hogy a potenciálisan kártékony művelet hogyan történhet meg az eszközön, ezért nem teljesen hasonlítható olyan kategóriákhoz, mint a számlázási csalás vagy a kereskedelmi kémprogramok. A Google Play Protect emiatt bizonyos esetekben sebezhetőségként kezel egyes hátsó ajtókat.

Számlázási csalás

Olyan kód, amely szándékosan csalárd módon és automatikusan terheli meg a felhasználó fizetési módját.

A mobilszámlázási csalásnak három fajtája van: SMS-sel elkövetett, hívással elkövetett, illetve előfizetéses.

SMS-sel elkövetett csalás
Olyan kód, amely a felhasználó beleegyezése nélkül emelt díjas SMS-eket küld, vagy úgy próbálja meg leplezni SMS-küldési tevékenységét, hogy elrejti azokat a beleegyezési nyilatkozatokat vagy SMS-eket a felhasználó elől, amelyekben a mobilszolgáltató értesíti a felhasználót a terhelésekről vagy az előfizetések elfogadásáról.

Bizonyos kódok, még ha gyakorlatilag tájékoztatást is adnak az SMS-küldési viselkedésükről, egyéb viselkedést is megvalósítanak, amely kimeríti az SMS-sel elkövetett csalás fogalmát. Ilyen például, ha a kód olvashatatlanná teszi, elrejti a beleegyezési nyilatkozat egyes részeit a felhasználó elől, vagy ha bizonyos feltételek teljesülése esetén elrejti a mobilszolgáltatótól érkező olyan üzeneteket, amelyek tájékoztatnák a felhasználót a terhelésekről vagy az előfizetések elfogadásáról.

Hívással elkövetett csalás
Olyan kód, amely azzal terheli meg a felhasználók fizetési módját, hogy emelt díjas számokat hív a felhasználók beleegyezése nélkül.

Előfizetéses csalás
Olyan kód, amely ráveszi a felhasználókat arra, hogy mobilszámlájuk terhére előfizetést indítsanak, vagy vásárlást hajtsanak végre.

Előfizetéses csalásnak minősül minden mobilfizetéses csalás, amely nem emelt díjas SMS vagy hívás formáját ölti. Ilyen például a közvetlen mobilszámlázással való visszaélés, valamint a vezeték nélküli hozzáférési pontok (WAP) és a mobilinternet engedély nélküli használata. A WAP-csalás az egyik leggyakoribb előfizetéses csalás. WAP-csalás lehet például az is, ha a felhasználókat ráveszik, hogy egy észrevétlenül betöltött, átlátszó WebView-ra kattintsanak. Kattintás után a rendszer megújuló

előfizetést kezdeményez, a támadó pedig gyakran eltéríti a visszaigazoló SMS-t vagy e-mailt, hogy a felhasználó ne vegye észre a pénzügyi tranzakciót.

Stalkerware

Az eszközről személyes vagy bizalmas felhasználói adatot gyűjtő és a gyűjtött adatokat felügyeleti célokra harmadik fél (vállalat vagy más magánszemély) részére továbbító kód.

Az alkalmazásoknak a felhasználói adatokra vonatkozó irányelvek által előírt módon megfelelő, jól láthatóan elhelyezett nyilatkozatot kell közölniük, és beleegyezést kell szerezniük.

A felügyeleti tevékenységet végző alkalmazásokra vonatkozó irányelvek

Kizárólag azok az elfogadható felügyeleti alkalmazások, amelyek egy másik személy felügyeletére szolgálnak, így is kerülnek forgalomba (például szülők számára gyermekük megfigyeléséhez vagy vállalatok irányítása számára az egyes munkavállalók felügyeletéhez), és teljes mértékben megfelelnek az alábbiakban ismertetett követelményeknek. Ezekkel az alkalmazásokkal mások (például házastárs) nem követhető nyomon, még a tudtukkal és a hozzájárulásukkal sem, függetlenül attól, hogy egy folyamatosan látható értesítés jelenik meg. Az ilyen alkalmazásoknak az IsMonitoringTool metadat-jelölőt kell használniuk manifestfájljukban, hogy így megfelelőképpen sorolják be magukat felügyeleti alkalmazásként.

A felügyeleti alkalmazásoknak a következő követelményeknek kell megfelelniük:

- Nem tüntethetik fel magukat kémkedést vagy titkos megfigyelést elősegítő megoldásként.
- Nem rejthetik el vagy álcázhatják a követési tevékenységüket, és nem vezethetik félre a felhasználókat az ilyen jellegű működésükkel kapcsolatban.
- Az alkalmazásoknak működés közben egy folyamatosan látható értesítést és ikont kell megjeleníteni, amely alapján egyértelműen beazonosítható az adott alkalmazás.
- A Google Play Áruházban az alkalmazások leírásában közölni kell, hogy az adott alkalmazás felügyeletre vagy nyomon követésre szolgál.
- A Google Playen található alkalmazások és áruházi adatlapjaik nem adhatnak módot olyan funkciók aktiválására vagy elérésére, amelyek sértik ezeket a feltételeket. Ilyen például a Google Playen kívül tárolt, nem megfelelő APK-ra mutató hivatkozás.
- Az alkalmazásoknak valamennyi vonatkozó jogszabálynak meg kell felelniük. Teljes mértékben a te feladatod, hogy megállapítsd az alkalmazás jogszerűségét a megcélzott országban vagy területen.

További információért olvasd el Az isMonitoringTool jelző használata című súgócikket.

Szolgáltatásmegtagadással járó támadás (DoS)

Olyan kód, amely a felhasználó tudomása nélkül szolgáltatásmegtagadással járó (DoS) támadást hajt végre, vagy más rendszerek és erőforrások ellen irányuló elosztott szolgáltatásmegtagadó támadásban vesz részt.

Ezt például nagy mennyiségű HTTP-kérés küldésével lehet elérni, ami túlzottan nagy terhelést eredményez a távoli szerveren.

Ellenséges letöltők

Olyan kód, amely önmagában nem kártékony, de más potenciálisan kártékony alkalmazásokat tölt le.

A kód ellenséges letöltő lehet, ha:

- indokoltan feltételezhető, hogy potenciálisan kártékony alkalmazások terjesztésére hozták létre, és le is töltött ilyen alkalmazásokat, vagy olyan kódot tartalmaz, amely letölthet és telepíthet alkalmazásokat; vagy
- az általa letöltött alkalmazások legalább 5%-a potenciálisan kártékony alkalmazás, és legalább 500 megfigyelt alkalmazásletöltés volt (ez 25 potenciálisan kártékony alkalmazás letöltését jelenti).

Az elterjedtebb böngészők és fájlmegosztó alkalmazások nem minősülnek ellenséges letöltőknek, ha:

- nem kezdeményeznek letöltéseket felhasználói interakció nélkül; és
- a potenciálisan kártékony alkalmazások letöltését a beleegyezését adó felhasználó kezdeményezte.

Androidra nem veszélyes fenyegetés

Az Androidra nem veszélyes fenyegetést tartalmazó kód.

Ezek az alkalmazások nem tudnak ártani az Android-eszközöknek és felhasználóiknak, de olyan komponenseik vannak, amelyek kártékonyak lehetnek más operációs rendszereken.

Adathalászat

Olyan kód, amely úgy tesz, mintha megbízható forrásból származna, elkéri a felhasználó hitelesítési vagy számlázási adatait, majd az adatokat harmadik félnek továbbítja. Ebbe a kategóriába tartoznak azok a kódok is, amelyek a felhasználó hitelesítési adatait továbbítás közben szerzik meg.

Az adathalászat gyakori célpontjai a banki hitelesítési adatok, a hitelkártyaszámok, valamint a közösségi oldalakhoz és online játékokhoz tartozó fiókhitelesítési adatok.

Visszaélés magasabb szintű hozzáféréssel

Olyan kód, amely károsítja a rendszer integritását például úgy, hogy megakadályozza az alkalmazásfuttató sandbox megfelelő működését, magasabb szintű rendszerhozzáférésre tesz szert, módosítja vagy letiltja az alapvető biztonsági funkciók hozzáférhetőségét.

Ilyenek például a következők:

- olyan alkalmazások, amelyek áthágják az Android engedélykezelő rendszerét, vagy hitelesítési adatokat (pl. OAuth-tokeneket) szereznek más alkalmazásoktól;
- olyan alkalmazások, amelyek saját eltávolításuk vagy leállításuk megakadályozása érdekében visszaélnek bizonyos funkciókkal;
- olyan alkalmazások, amelyek letiltják a SELinux modult.

Magasabb szintű hozzáférést szerző alkalmazások, amelyek a felhasználó engedélye nélkül rootolják az eszközt – ezeket rootoló alkalmazásoknak nevezzük.

Zsarolóprogram

Olyan kód, amely részleges vagy teljes irányítása alá vonja az eszközt vagy az eszközön tárolt adatokat, majd ennek visszavonásáért pénz kifizetésére vagy valamilyen művelet végrehajtására kényszeríti a felhasználót.

Bizonyos zsarolóprogramok titkosítják az eszközön tárolt adatokat, majd pénzt követelnek a titkosítás visszavonásáért, valamint az eszköz rendszergazdai funkcionalitását kihasználva megakadályozhatják, hogy az átlagos ismeretekkel rendelkező felhasználó eltávolítása őket. Ilyenek például a következők:

- az eszközhöz való hozzáférés megvonása a felhasználótól, majd pénz követelése a hozzáférés visszaállításáért;
- az eszköz adatainak titkosítása, majd pénz követelése a titkosítás állítólagos megszüntetéséért;
- az eszköz házirendkezelőjének kihasználása és a felhasználó általi eltávolítás megakadályozása.

Kivételt tehetünk olyan eszközzel együtt terjesztett kódok esetében, melyek elsődleges célja, hogy más felek általi eszközfelügyeletet tegyen lehetővé. A kivétel feltétele, hogy a kód megfeleljen a biztonságos zároláshoz és kezeléshez szükséges követelményeknek, megfelelő tájékoztatást nyújtson a felhasználónak, valamint megfelelő beleegyezést kérjen tőle.

Rootolás

Olyan kód, amely rootolja az eszközt.

Különbség van a nem rosszindulatú és a rosszindulatú rootolási kódok között. A nem rosszindulatú rootoló alkalmazások például előre tájékoztatják a felhasználót arról, hogy rootolni fogják az eszközt, és nem hajtanak végre egyéb potenciálisan kártékony kategóriákba tartozó műveletet sem.

A rosszindulatú rootoló alkalmazások nem tájékoztatják előre a felhasználót arról, hogy rootolni fogják az eszközt, vagy tájékoztatják róla, de egyúttal végrehajtanak más kártékony műveleteket is, amelyek egyéb potenciálisan kártékony kategóriákba tartoznak.

Spam

Olyan kód, amely kéretlen üzeneteket küld a felhasználó ismerőseinek, vagy a felhasználó eszközét használja fel spamjellegű e-mailek továbbítására.

Kémprogram

A kémprogram olyan rosszindulatú alkalmazás, kód vagy viselkedés, amely olyan felhasználói vagy eszközadatokat gyűjt, juttat ki vagy oszt meg, amelyek nem a házirendnek megfelelő funkciókhoz kapcsolódnak.

Kémprogramnak minősül az a rosszindulatú kód vagy viselkedés is, amellyel kapcsolatban fontolóra vehető, hogy a felhasználó után kémkedik, vagy pedig megfelelő értesítés vagy beleegyezés nélkül juttat ki adatokat.

Kémprogrammal való irányelvsértés többek között például a következő:

- A hangrögzítés, a telefonon lebonyolított hívások rögzítése
- Az alkalmazások adatainak ellopása
- A rosszindulatú, harmadik féltől származó kódot (például SDK-t) tartalmazó alkalmazás, amely a felhasználó számára váratlan módon és/vagy a felhasználó megfelelő értesítése vagy beleegyezése nélkül továbbít adatot az eszközről.

Valamennyi alkalmazásnak meg kell felelnie továbbá minden Google Play Fejlesztői Programszabályzatnak, így például a felhasználói és az eszközadatokra vonatkozó irányelveknek, például a nemkívánatos mobilszoftverekre, a felhasználói adatokra, az engedélyekre és a bizalmas információhoz hozzáférő API-kra vonatkozó irányelvnek, továbbá az SDK-követelményeknek.

Trójai program

Ártalmatlannak tűnő kód, például egy olyan játék, amely egyegyszerű játéknak tünteti fel magát, de a felhasználó számára nemkívánatos műveleteket hajt végre.

Ezt a besorolást általában a potenciálisan kártékony alkalmazások (PHA) egyéb kategóriával együtt használjuk. A trójai kártevők ártalmatlan részből és rejtett kártékony összetevőből állnak. Ilyen például az a játék, amely a háttérben emelt díjas SMS-eket küld az eszközről, a felhasználó tudta nélkül.

Megjegyzés a szokatlan alkalmazásokkal kapcsolatban

Szokatlanként jelölhetjük meg az új és ritka alkalmazásokat, ha a Google Play Protect nem rendelkezik elég információval biztonságos jellegük megállapításához. Ez nem jelenti azt, hogy az alkalmazás mindenképpen kártékony, de további ellenőrzés nélkül nem jelenthető ki róla az sem, hogy biztonságos.

Megjegyzés a hátsó ajtó kategóriával kapcsolatban

A rosszindulatú programok „hátsó ajtó” kategóriájába való besorolás a kód viselkedésén alapul. A hátsó ajtóként való besorolás szükséges feltétele, hogy a kód olyan viselkedést tegyen lehetővé, amely automatikus végrehajtás esetén a kódot más fajta rosszindulatú programnak minősítené. Például ha az

alkalmazás dinamikus kódbetöltést tesz lehetővé, és a dinamikusan betöltött kód engedély nélkül hozzáfér a szöveges üzenetekhez, akkor hátsó ajtóról beszélünk.

Mindazonáltal ha az alkalmazás ugyan tetszőleges kód végrehajtását teszi lehetővé, de nincs okunk azt feltételezni, hogy ezt a lehetőséget rosszindulatú viselkedés megvalósítása miatt helyezték el, akkor az alkalmazást sebezhetőséggel rendelkező szoftvernek tekintjük, nem pedig hátsó ajtó típusú rosszindulatú programnak – és megkérjük a fejlesztőt, hogy javítsa a sebezhetőséget.

Maszkolóprogram (maskware)

Olyan alkalmazás, amely különböző kijátszási technikákat alkalmaz annak érdekében, hogy a felhasználónak más vagy hamis alkalmazási funkciókat kínáljon. Ezek az alkalmazások legitim alkalmazásoknak vagy játékoknak álcázzák magukat, hogy ártalmatlannak tűnjenek az alkalmazásboltok számára, és olyan technikákat használnak, mint az érthetetlenné tétel (obfuszkálás), a dinamikus kódbetöltés vagy az álcázás, hogy szabadon engedjék a rosszindulatú tartalmat.

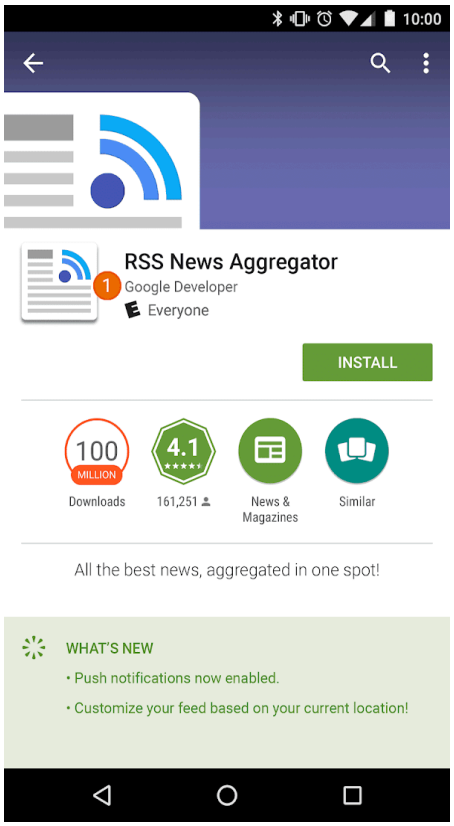
A maszkolóprogram (maskware) hasonló más PHA-kategóriákhoz, különösen a trójaiakhoz; a fő különbség a rosszindulatú tevékenység obfuszkálására használt technikákban rejlik.

Mások személyi adataival való visszaélés

Nem engedélyezünk olyan alkalmazásokat, amelyek félrevezetik a felhasználókat úgy, hogy valaki másnak (pl. másik fejlesztő, vállalkozás, jogi személy) vagy más alkalmazásnak adják ki magukat. Ne utaljon arra, hogy az alkalmazás valamilyen személyhez kapcsolódik, vagy valaki jóváhagyását élvezi, ha ez nem igaz. Ne használjon olyan alkalmazásikonokat, leírásokat, címeket vagy alkalmazáson belüli elemeket, amelyek alapján a felhasználók tévesen azt hihetik, hogy az alkalmazás valamilyen személlyel vagy más alkalmazással áll kapcsolatban.

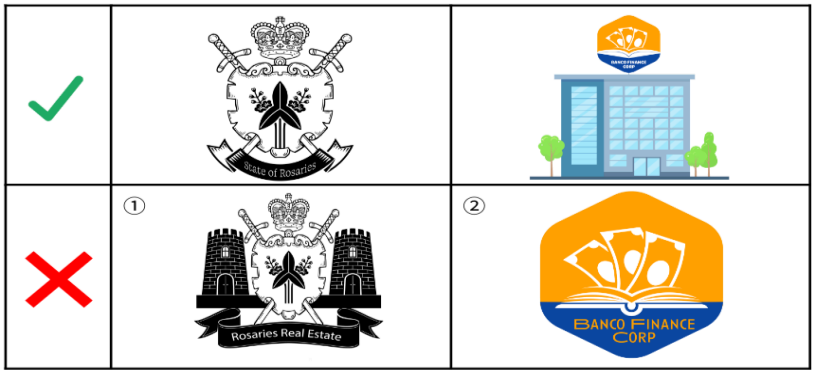
Néhány példa a gyakori irányelvsértésekre:

- Fejlesztők, akik hamisan sugallják, hogy kapcsolatban állnak egy másik vállalkozással vagy fejlesztővel.



① Az alkalmazás mellett a fejlesztő neve azt sugallja, hogy hivatalos kapcsolatban áll a Google-lal, noha ilyen kapcsolat nem áll fenn.

- Alkalmazások, amelyek ikonjai és címei hamisan sugallják a más céggel/fejlesztővel/entitással/szervezettel fennálló kapcsolatot.



① Az alkalmazás nemzeti jelképet használ, félrevezetve ezzel a felhasználókat, akik úgy vélhetik, hogy az alkalmazás az adott államhoz kapcsolódik.
②Az alkalmazás egy üzleti entitás logóját másolja, hamisan sugallva ezzel azt, hogy az adott üzleti vállalkozás hivatalos alkalmazása.

- Olyan alkalmazáscímek és -ikonok, amelyek más termékek vagy szolgáltatások címére vagy ikonjára hasonlítanak, ezért félrevezethetik a felhasználókat.

①Alkalmazásikonjában az alkalmazás valamely népszerű kriptovaluta webhelyének logóját használja, azt sugallva ezzel, hogy az a hivatalos webhelye.
②Alkalmazásikonjában az alkalmazás egy híres tévéműsor valamelyik szereplőjét és a műsor címét másolja, félrevezetve ezzel a felhasználókat, akik úgy vélhetik, hogy az alkalmazás az adott tévésműsorhoz kapcsolódik.

- Alkalmazások, amelyek hamisan állítják, hogy valamely ismert szervezet vagy személy hivatalos alkalmazásai. A szükséges engedélyek és jogok nélkül tilos olyan címeket adni, mint például a „Justin Bieber hivatalos alkalmazása”.
- Alkalmazások, amelyek sértik az Android márkajegyhasználati irányelveit .

Nemkívánatos mobilszoftverek

A Google-nál úgy hisszük, hogy ha a felhasználókra koncentrálunk, akkor minden másra is odafigyelünk. A szoftverre vonatkozó irányelvekben és a nemkívánatos szoftverekre vonatkozó irányelvekben olyan általános javaslatokat teszünk közzé a szoftverekkel kapcsolatban, amelyek jó felhasználói élményt biztosítanak. Ez az irányelv a Google nemkívánatos szoftverekre vonatkozó irányelveinek alapján határozza meg az Android-ökoszisztéma és a Google Play Áruház alapelveit. Az alábbi alapelveket megsértő szoftverek károsak lehetnek a felhasználói élmény szempontjából, ezért megtesszük a megfelelő lépéseket, hogy felhasználóinkat megóvjuk tőlük.

Amint ezt a nemkívánatos szoftverekről szóló irányelvekben is említettük, tapasztalataink szerint a legtöbb nemkívánatos szoftver a következő alapvető jellemzők legalább egyikével rendelkezik:

- Csalárd, mert olyan értékajánlatot ígér, amelyet nem tud teljesíteni.
- Megpróbálja rávenni a felhasználókat a telepítésre, vagy egy másik programhoz kapcsolódóan települ.
- Nem árul el mindent a felhasználónak az alapvető és lényeges funkciókról.
- Nem várt módon befolyásolja a felhasználó rendszerét.
- A felhasználó tudta nélkül magánjellegű információkat gyűjt vagy továbbít.
- Magánjellegű információkat gyűjt vagy továbbít biztonságos kezelés (pl. HTTPS-kapcsolat) nélkül.
- Más szoftverrel együtt terjed, és nem tájékoztat a jelenlétéről.

Mobileszközökön a szoftverek olyan kódok, amelyek alkalmazás, bináris program, keretrendszer-módosítás stb. formáját öltik. Az alapelveinket sértő kódok esetében megfelelő lépéseket teszünk, hogy megakadályozzuk az olyan szoftverek terjedését, amelyek károsak szoftver-ökoszisztémánkra, vagy zavarók a felhasználói élmény szempontjából.

Az alábbiakban a nemkívánatos szoftverekről szóló irányelveinket terjesztjük ki a mobilszoftverekre. Ahogyan az eredeti irányelveket, a nemkívánatos mobilszoftverekről szóló irányelveinket is frissítjük majd, hogy lefedjék a későbbiekben felfedezett visszaélésfajtákat is.

Átlátható viselkedés és egyértelmű tájékoztatás

Minden kódnak teljesítenie kell a felhasználóknak tett ígéreteket. Az alkalmazásoknak minden bemutatott funkciót biztosítaniuk kell. Az alkalmazásoknak nem szabad összezavarniuk a felhasználókat.

- Az alkalmazások funkcióinak és céljainak egyértelműnek kell lenniük.
- Egyértelműen és pontosan el kell magyarázni a felhasználónak, hogy az alkalmazás milyen rendszermódosításokat hajt végre. Tegye lehetővé a felhasználók számára az összes fontos telepítési lehetőség és módosítás áttekintését és jóváhagyását.
- A szoftver nem közölhet valótlan információt az eszköz állapotáról a felhasználóval, például nem állíthatja hamisan azt, hogy a rendszer biztonsági állapota kritikus, vagy hogy a rendszer vírusokkal fertőzött.
- Ne használjon érvénytelen tevékenységeket, amely célja a hirdetési forgalom és/vagy a konverziók számának növelése.
- Nem engedélyezünk olyan alkalmazásokat, amelyek félrevezetik a felhasználókat úgy, hogy valaki másnak (pl. másik fejlesztő, vállalkozás, jogi személy) vagy más alkalmazásnak adják ki magukat. Ne utaljon arra, hogy az alkalmazás valamilyen személyhez kapcsolódik, vagy valaki jóváhagyását élvezi, ha ez nem igaz.

Néhány irányelvsértés:

- Hirdetési csalás
- Bizalomra épülő manipuláció

A felhasználói adatok védelme és az adatvédelem

A személyes és bizalmas felhasználói adatokhoz való hozzáférésnek, valamint az ilyen adatok használatának, gyűjtésének és megosztásának egyértelműnek és átláthatónak kell lennie. A felhasználói adatok felhasználása során az összes vonatkozó irányelvet követni kell, és meg kell tenni minden óvintézkedést az adatok védelme érdekében.

Az összes alkalmazásnak meg kell felelnie minden Google Play Fejlesztői Programszabályzatnak, így például a felhasználói és az eszközadatokra vonatkozó irányelveknek, például a felhasználói adatokra, engedélyekre és a bizalmas információhoz hozzáférő API-kra, továbbá a kémprogramokra vonatkozó irányelvnek, valamint az SDK-követelményeknek.

- Ne kérd és ne vedd rá arra a felhasználókat, hogy kapcsolják ki az eszköz biztonsági védelmét, például a Google Play Protectet. Például nem kínálhatsz további alkalmazásfunkciókat vagy jutalmakat a felhasználóknak a Google Play Protect kikapcsolásáért cserébe.

Ne rontsa a mobilos élményt

A felhasználói élménynek értelemszerűnek és könnyen érthetőnek kell lennie, valamint a felhasználó egyértelmű választásán kell alapulnia. Világosan közölt értékajánlatot kell kínálnia a felhasználónak, és nem zavarhatja a hirdetett vagy a kívánt felhasználói élményt.

- Ne jelenítsen meg olyan hirdetéseket, amelyek váratlan módon jelennek meg a felhasználóknak, hátrányosan befolyásolják vagy zavarják az eszköz funkcióinak használhatóságát, az őket aktiváló alkalmazás környezetén kívül jelennek meg anélkül, hogy könnyen elvethetők lennének, vagy amelyeknél hiányzik a megfelelő hozzájárulás és megjelölés.
- Az alkalmazások nem zavarhatják a többi alkalmazást, sem az eszköz használhatóságát.
- Az alkalmazás eltávolításának adott esetben egyértelműnek kell lennie.
- A mobilszoftver nem utánozhatja az eszköz operációs rendszerétől vagy más alkalmazásoktól származó értesítéseket. Ne rejtse el a felhasználó elől a más alkalmazásokból vagy az operációs rendszertől érkező értesítéseket, különös tekintettel azokra, amelyek az operációs rendszer módosításairól tájékoztatják a felhasználót.

Néhány irányelvsértés:

- Zavaró hirdetések
- Illetéktelen használat és rendszerműködés utánzása

Ellenséges letöltők

Olyan kód, amely önmagában nem nemkívánatos szoftver, de más nemkívánatos mobilszoftvereket (MUwS) tölt le.

A kód ellenséges letöltő lehet, ha:

- indokoltan feltételezhető, hogy nemkívánatos mobilszoftverek terjesztésére hozták létre, és le is töltött ilyen alkalmazásokat, vagy olyan kódot tartalmaz, amely letölthet és telepíthet alkalmazásokat; vagy
- az általa letöltött alkalmazások legalább 5%-a nemkívánatos mobilszoftver, és legalább 500 megfigyelt alkalmazásletöltés volt (ez 25 nemkívánatos mobilszoftver letöltését jelenti).

Az elterjedtebb böngészők és fájlmegosztó alkalmazások nem minősülnek ellenséges letöltőknek, ha:

- nem kezdeményeznek letöltéseket felhasználói interakció nélkül; és
- a szoftver letöltését a beleegyezését adó felhasználó kezdeményezte.

Hirdetési csalás

A hirdetési csalás szigorúan tilos. Hirdetési csalásnak minősülnek azok a hirdetési interakciók, amelyeknek az a célja, hogy a hirdetési hálózattal elhitessék, hogy a forgalom valódi felhasználói

érdeklődésen alapul – ez az érvénytelen forgalom egyik formája. A hirdetési csalás annak a melléktermeke lehet, hogy a fejlesztők nem engedélyezett módon valósítanak meg hirdetéseket. Ide tartozik például a rejtett hirdetések megjelenítése, az automatikus kattintás a hirdetésekre, az információk módosítása, illetve a nem emberi műveletek (robotok, botok stb.) más módon történő kihasználása, valamint az érvénytelen hirdetésforgalom generálását szolgáló emberi tevékenységek. Az érvénytelen forgalom és a hirdetési csalások károsak a hirdetők, a fejlesztők és a felhasználók számára, és a mobilhirdetések ökoszisztémájába vetett bizalom hosszú távú elvesztéséhez vezetnek.

Néhány példa a gyakori irányelvsértésekre:

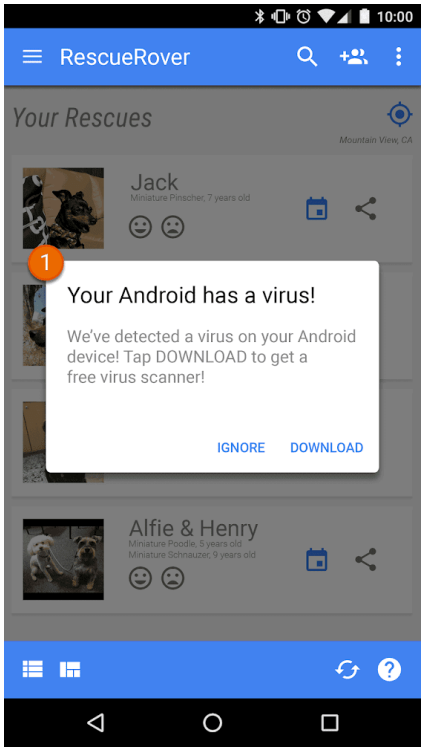
- olyan alkalmazás, amely a felhasználó számára nem látható hirdetéseket jelenít meg;
- olyan alkalmazás, amely automatikusan hirdetésre leadott kattintásokat generál a felhasználó szándéka nélkül, vagy olyan hálózati forgalmat generál, amely csalárd módon eredményez kattintási jóváírást;
- olyan alkalmazás, amely hamis telepítésindítási kattintásokat küld, hogy pénzt kapjon olyan telepítésekért, amelyek nem a küldő hálózatáról származnak;
- olyan alkalmazás, amely előugró hirdetéseket jelenít meg, amikor a felhasználó nem az alkalmazás kezelőfelületét használja;
- a hirdetéskészletre vonatkozó megtévesztés (pl. az alkalmazás azt kommunikálja a hirdetési hálózatok számára, hogy iOS-eszközön fut, de a valóságban Androidon); olyan alkalmazások, amelyek hamisan tüntetik fel a bevételszerzésre használt csomagnevet.

Illetéktelen használat és rendszerműködés utánzása

Nem engedélyezzük azokat az alkalmazásokat vagy hirdetéseket, amelyek utánozzák vagy zavarják a rendszerfunkciókat, például az értesítéseket vagy figyelmeztetéseket. A rendszerszintű értesítéseket csak az alkalmazás által biztosított belső funkciókhoz lehet használni. Ilyen például, amikor egy légitársaság alkalmazása rendkívüli ajánlatokról, vagy amikor egy játék a játékon belüli promóciókról értesíti a felhasználókat.

Néhány példa a gyakori irányelvsértésekre:

- Rendszerértesítés vagy -riasztás használatával megjelenített alkalmazások vagy hirdetések:



① Az alkalmazás által használt rendszerértesítésben hirdetést jelenítenek meg.

További hirdetésekkel kapcsolatos példák találhatók a hirdetésekre vonatkozó irányelvekben.

Bizalomra épülő manipuláció

Nem engedélyezünk olyan alkalmazásokat, amelyek másik alkalmazásnak adják ki magukat azzal a céllal, hogy megtévesztés révén rávegyék a felhasználókat olyan műveletek végrehajtására, amelyeket az eredeti, megbízható alkalmazással szerettek volna végrehajtani.

Bevételszerzés és hirdetések

A Google Play többféle, a fejlesztők és felhasználók előnyére szolgáló bevételszerzési stratégiát támogat, így például a fizetett terjesztést, az alkalmazáson belüli termékeket, az előfizetéseket és a hirdetésalapú modelleket. A legjobb felhasználói élmény biztosítása érdekében a fejlesztőknek be kell tartaniuk ezeket az irányelveket.

Fizetés

1. A Google Play felületén alkalmazásletöltésekért díjat felszámító fejlesztőknek a Google Play számlázási rendszerét kell használniuk a fizetés módjaként az ilyen tranzakciók esetében.
2. A Play felületén terjesztett olyan alkalmazások esetében, amelyek fizetést igényelnek vagy fogadnak el az alkalmazáson belüli funkciókhoz vagy szolgáltatásokhoz, beleértve az alkalmazásfunkciókat, a digitális tartalmakhoz vagy az árucikkekhez való hozzáférés érdekében (együttesen mint „alkalmazáson belüli vásárlások”), a Google Play számlázási rendszerét kell használni, kivéve, ha a tranzakciókra a 3., a 8. vagy a 9. szakasz vonatkozik.

   Példák olyan alkalmazáson belüli vásárlásokra, melyekhez kapcsolódóan az alkalmazásfunkciók vagy szolgáltatások a Google Play számlázási rendszerét igénylik:

   - digitális elemek (például virtuális pénz, plusz élet, plusz játékidő, kiegészítő tárgyak, karakterek és avatarok);
   - előfizetéses szolgáltatások (például fitnesz-, játék-, társkereső, oktatási, zenés, videós és egyéb, előfizetéshez kötött tartalomszolgáltatások, illetve szolgáltatásbővítés);
   - alkalmazásfunkció vagy -tartalom (például az alkalmazás hirdetésmentes verziója, vagy a díjmentes változatban nem nyújtott új funkciók);
   - felhőalapú szoftverek és szolgáltatások (például adattárolási szolgáltatások, irodai programcsomagok és pénzügyimenedzsment-szoftverek).

3. A Google Play számlázási rendszere nem használható olyan esetben, amikor:
   a. a fizetés célja elsődlegesen:
      - fizikai termékek (például élelmiszerek, ruházat, háztartási és elektronikai eszközök) vásárlása vagy kölcsönzése;
      - fizikai szolgáltatások (például utazási, takarítási szolgáltatások, légi közlekedés, edzőtermi belépők, házhozszállítás, élő előadásokra szóló jegyek stb.) vásárlása; vagy
      - átutalás hitelkártyaszámlával vagy közüzemi számlával kapcsolatban (például kábel- vagy telekommunikációs szolgáltatások);
   b. peer-to-peer kifizetés, online aukció vagy adómentes adomány is szerepel a kifizetések között;
   c. a fizetés olyan tartalomért vagy szolgáltatásért cserébe történik, amely online szerencsejátékot segít elő (az online szerencsejátékok meghatározása a valódi pénzzel játszott

szerencsejátékokra, játékokra és versenyekre vonatkozó irányelvünk Szerencsejáték-alkalmazások szakaszában olvasható);

d. a fizetés olyan termékkategóriával kapcsolatos, amely elfogadhatatlannak minősül a Google fizetési központ tartalmi irányelvei értelmében.

> Megjegyzés: Bizonyos piacokon a Google Pay használható olyan alkalmazásoknál, amelyek fizikai termékeket és/vagy szolgáltatásokat kínálnak. További információt a Google Pay fejlesztői oldalán találhatsz.

4. A 3., a 8. és a 9. szakaszban ismertetett feltételek kivételével az alkalmazások kizárólag a Google Play számlázási rendszerébe irányíthatják át a felhasználókat fizetéskor. Idetartozik többek között az is, ha a felhasználókat a következőkön keresztül irányítják át más fizetési módokhoz:
   - az alkalmazás Google Playen található adatlapja;
   - megvásárolható tartalmakhoz kapcsolódó alkalmazáson belüli promóciók;
   - az alkalmazáson belüli WebView-k, gombok, linkek, üzenetek, hirdetések vagy más ösztönzések; és
   - alkalmazáson belüli kezelőfelületi folyamatok (például fióklétrehozási és regisztrációs folyamatok), amelyek a folyamat részeként az alkalmazásból a Google Play számlázási rendszerén kívüli fizetési módra vezetik a felhasználókat.
5. Az alkalmazáson belüli virtuális pénznemek használata kizárólag azon alkalmazáson vagy játékon belül megengedett, amelyben megvásárolták őket.
6. A fejlesztőknek világosan és pontosan tájékoztatniuk kell a felhasználókat az alkalmazás feltételeiről és árképzéséről, illetve az alkalmazáson belüli megvásárolható funkciókról és előfizetésekről. Az alkalmazáson belüli árképzésnek egyeznie kell a Play felhasználók számára megjelenő számlázási felületén látható árakkal. Ha az alkalmazás Google Playen szereplő leírása olyan alkalmazáson belüli funkciókat említ, amelyekhez meghatározott vagy plusz díj kifizetése szükséges, akkor az alkalmazás bolti adatlapjának egyértelműen tájékoztatnia kell a felhasználókat, hogy a funkciókhoz való hozzáférés fizetős.
7. Azon alkalmazásokban és játékokban, amelyekben véletlenszerű virtuális elemek vásárolhatók (például „loot boxok” formájában), egyértelműen fel kell tüntetni a véletlenszerű elemek megszerzésének esélyeit még a vásárlás előtt, de a vásárlás pillanatához a lehető legközelebb.
8. Hacsak a 3. szakaszban foglalt feltételek nem állnak fenn, a Play felületén terjesztett olyan alkalmazások fejlesztői, amelyek az alkalmazáson belüli vásárlásokhoz való hozzáférés érdekében fizetést kérnek vagy fogadnak el a felhasználóktól ezekben az országokban/régiókban, az alkalmazáson belül alternatív számlázási rendszert kínálhatnak fel a felhasználóknak a Google Play számlázási rendszere mellett az ilyen tranzakciók esetében, ha sikeresen kitöltik a számlázással kapcsolatos nyilatkozati űrlapot minden adott programra vonatkozóan, és elfogadják az abban foglalt további feltételeket és programkövetelményeket.
9. Előfordulhat, hogy a Playen terjesztett alkalmazások fejlesztői az Európai Gazdasági Térség (EGT) felhasználóit az alkalmazáson kívülre vezetik, többek között az alkalmazáson belüli digitális funkciók és szolgáltatások promóciós ajánlataihoz. Azoknak a fejlesztőknek, akik az EGT-beli felhasználókat az alkalmazáson kívülre vezetik, sikeresen ki kell tölteniük a programra vonatkozó nyilatkozati űrlapot, és el kell fogadniuk az abban foglalt további feltételeket és programkövetelményeket.

Megjegyzés: Az irányelvre vonatkozó határidők és a gyakori kérdések megtekintéséhez keresd fel a Súgót.

Hirdetések

A minőségi élmény fenntartása érdekében figyelembe vesszük a hirdetés tartalmát, célközönségét, felhasználói élményét, viselkedését, továbbá a biztonságot és az adatvédelmet. A hirdetéseket és a kapcsolódó ajánlatokat az alkalmazás részének tekintjük, így ezeknek is meg kell felelniük a Google

Play összes többi irányelvének. A hirdetésekre vonatkozóan további követelményeink is érvényesek, ha olyan alkalmazással szeretnél bevételt szerezni a Google Playen, amely gyermekeket céloz.

Az alkalmazáspromócióval és az áruházi adatlapokkal kapcsolatos irányelveinkről további információt találhatsz itt, beleértve azt is, hogy miként járunk el a megtévesztő promóciós gyakorlattal szemben.

Hirdetéstartalom

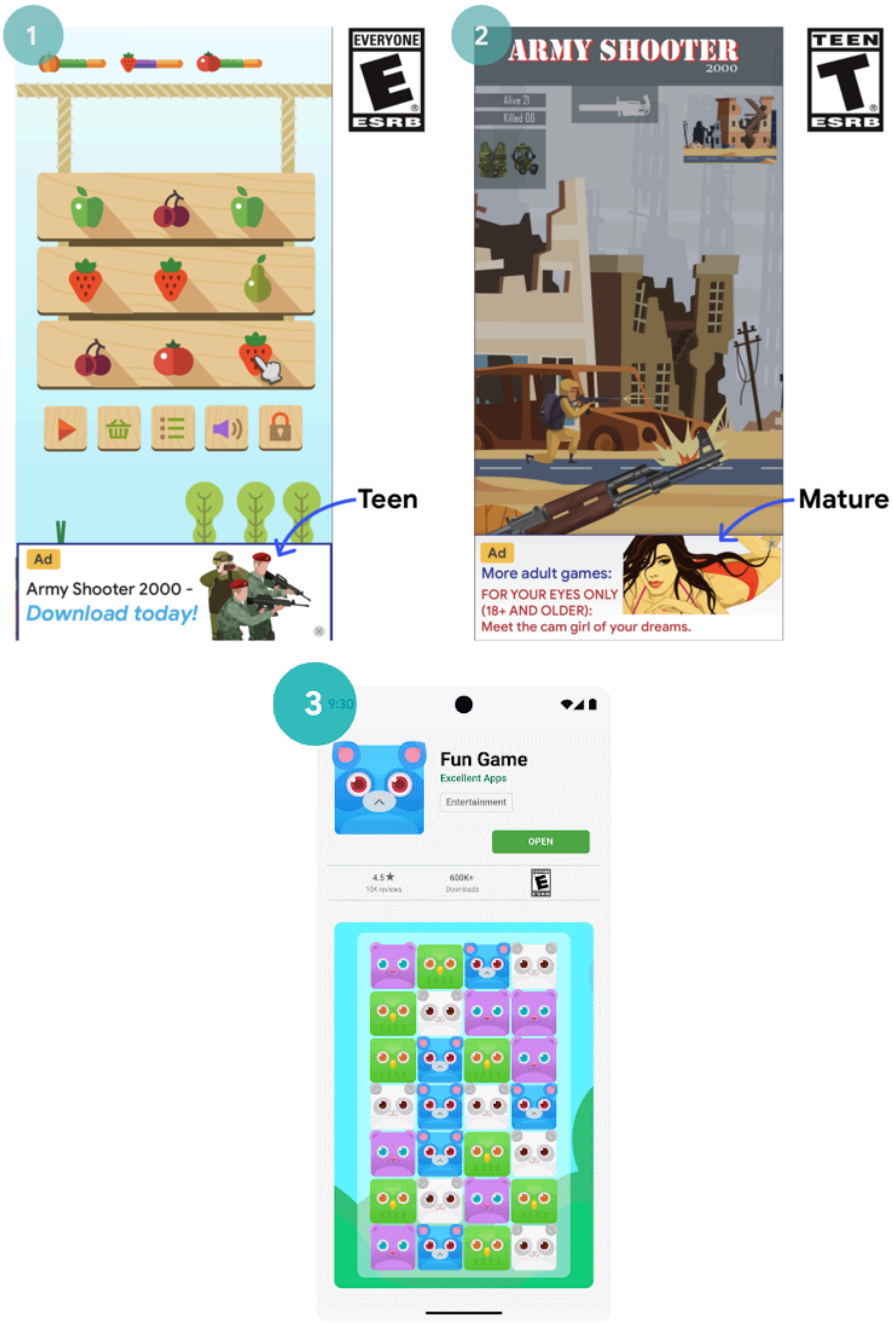
A hirdetések és a kapcsolódó ajánlatok az alkalmazásod részét képezik, és meg kell felelniük a korlátozott tartalomra vonatkozó irányelveinknek. Ha alkalmazásod szerencsejáték, akkor további követelmények érvényesek rá.

Nem megfelelő hirdetések

Az alkalmazásodon belül megjelenített hirdetéseknek és a hozzájuk társított ajánlatoknak (például amikor az alkalmazás egy másik alkalmazás letöltését népszerűsíti) illeszkedniük kell az alkalmazás tartalombesorolásához , még abban az esetben is, ha maga a tartalom egyébként megfelel az irányelveinknek.

Néhány példa a gyakori irányelvsértésekre:

- Az alkalmazás tartalmi besorolása szempontjából nem megfelelő hirdetések



① Ez a hirdetés nem felel meg (13 éven felülieknek) az alkalmazás tartalombesorolásának (Korhatár nélkül)
② Ez a hirdetés nem felel meg (Felnőtteknek) az alkalmazás tartalombesorolásának (13 éven felülieknek)
③ A hirdetés ajánlata (Felnőtteknek besorolású alkalmazás letöltését népszerűsíti) nem felel meg a hirdetést megjelenítő játékalkalmazás tartalombesorolásának (Korhatár nélkül)

Családi hirdetésekre vonatkozó előírások

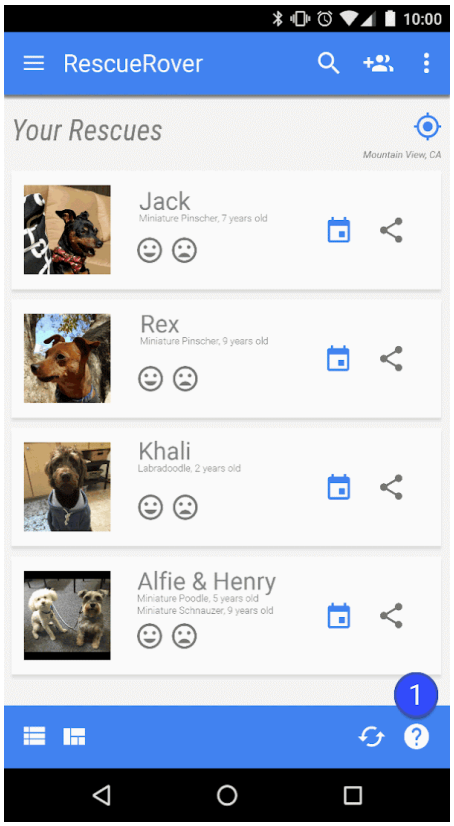
Ha olyan alkalmazásból történik a bevételszerzés a Google Playen, amely gyermekeket céloz, fontos, hogy az alkalmazás kövesse a Családokra vonatkozó hirdetésekkel kapcsolatos és bevételszerzési irányelveket.

Megtévesztő hirdetések

A hirdetések nem adhatják ki magukat más alkalmazás felhasználói felületének, illetve az operációs rendszer értesítéseinek vagy figyelmeztető elemeinek. Egyértelműnek kell lenni a felhasználó számára, hogy melyik alkalmazás jeleníti meg az egyes hirdetéseket.

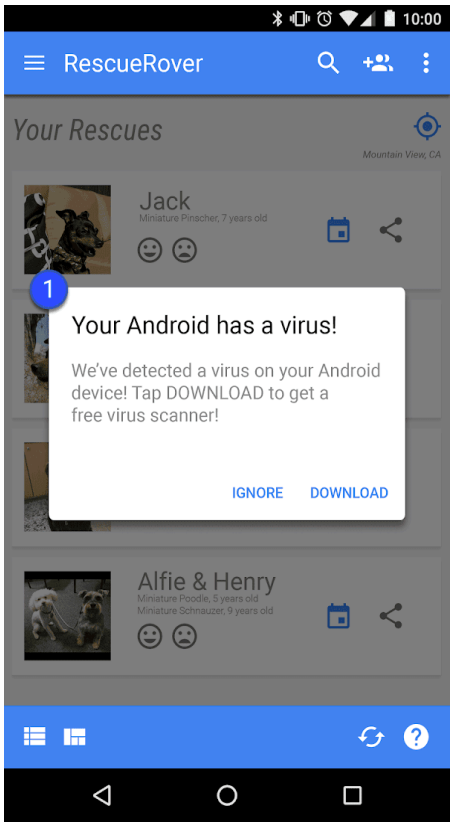
Néhány példa a gyakori irányelvsértésekre:

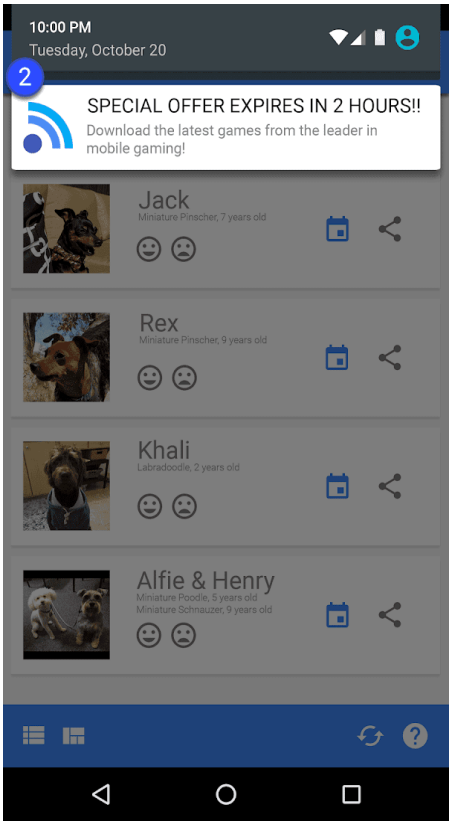
- Alkalmazás kezelőfelületét utánzó hirdetések:



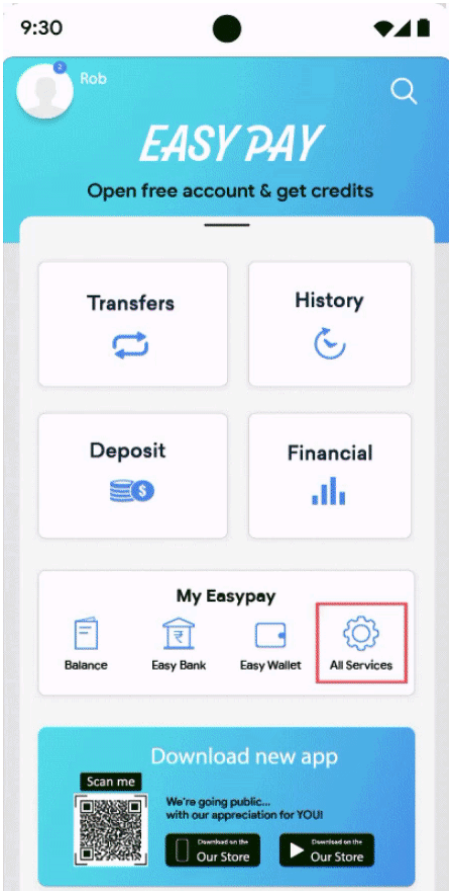
① Az alkalmazásban látható kérdőjel ikon egy hirdetés, amely a felhasználót egy külső céloldalra irányítja át.

- Rendszerértesítést utánzó hirdetések:





① ② A fenti példákban olyan hirdetések láthatók, amelyek különböző rendszerértesítéseket utánoznak.



① A fenti példa funkciók egy olyan menüjét illusztrálja, amely egyéb funkciókat utánoz, de csupán egy vagy több hirdetésre irányítja a felhasználót.

Zavaró hirdetések

Olyan hirdetéseket nevezünk zavarónak, melyek váratlan módon jelennek meg a felhasználók előtt, ezért véletlen kattintásokat eredményezhetnek vagy hátrányosan befolyásolhatják, zavarhatják az eszköz funkcióinak használhatóságát.

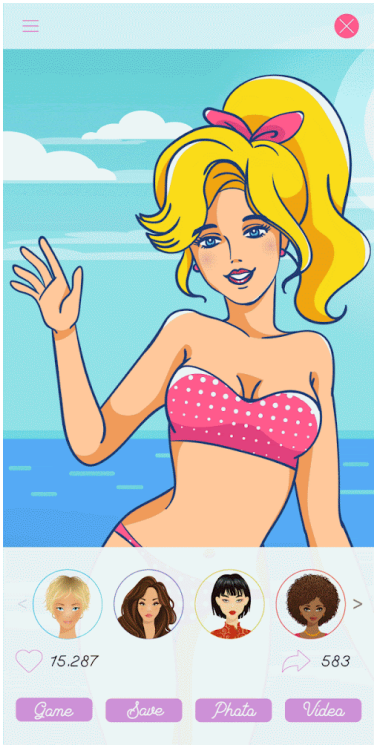
Tilos a felhasználót arra kényszeríteni, hogy az alkalmazás teljes használhatóságához hirdetésre kattintson, vagy hogy hirdetési célokra küldje be személyes adatait. A hirdetések csak a megjelenítésért felelős alkalmazáson belül jeleníthetők meg, és nem zavarhatnak más alkalmazásokat és hirdetéseket, sem az eszköz működését (például a rendszer vagy az eszköz gombjait és portjait). Idetartoznak a fedvények, a kísérőfunkciók, valamint a modulosított hirdetési egységek is. A rendeltetésszerű használatot megzavaró hirdetések csak akkor használhatók, ha könnyen és hátrány nélkül eltüntethetők.

Néhány példa a gyakori irányelvsértésekre:

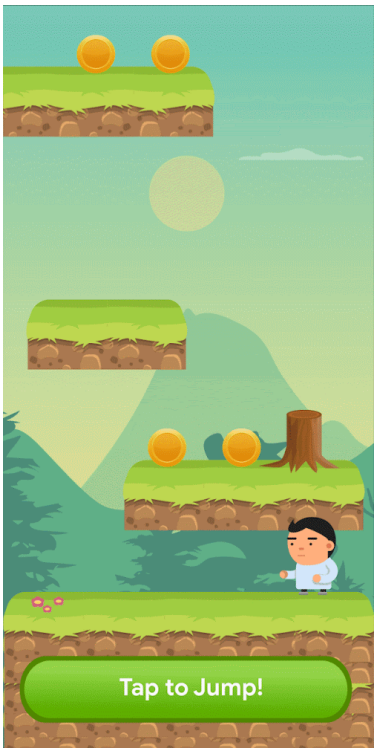
- Olyan hirdetések, amelyek elfoglalják a teljes képernyőt, illetve zavarják a rendeltetésszerű használatot, emellett nem biztosítanak a hirdetés bezárására vonatkozó egyértelmű jelölést:

① Ezen a hirdetésen nincsen bezárás gomb.

- Olyan hirdetések, amelyek átkattintásra kényszerítik a felhasználókat hamis Bezárás gombbal, vagy úgy, hogy hirtelen jelennek meg az alkalmazás olyan részén, ahová a felhasználó általában valamelyik másik funkció miatt koppint:

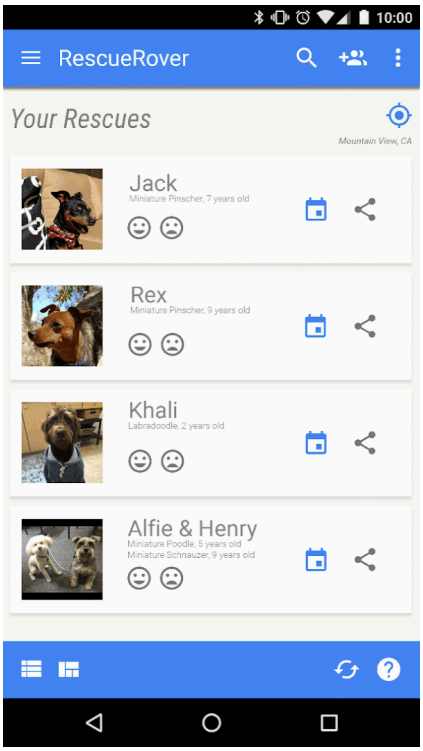


① Ez a hirdetés hamis Bezárás gombot használ.



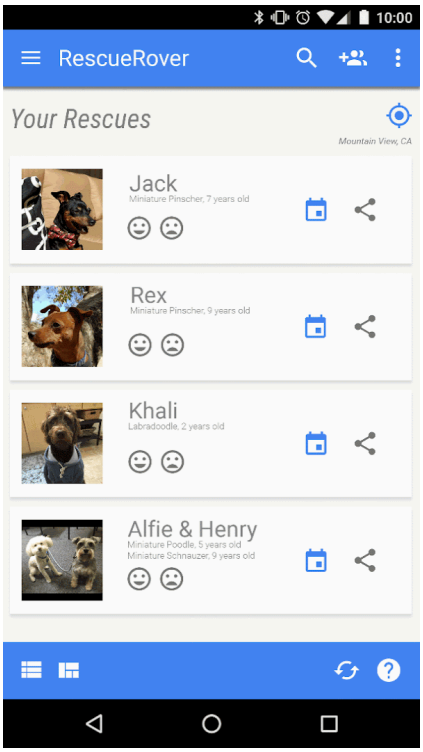
② Ez a hirdetés hirtelen jelenik meg egy olyan részen, ahová a felhasználó általában valamilyen alkalmazáson belüli funkció miatt koppint.

- Az alkalmazáson kívül megjelenő hirdetések:



① A felhasználó a kezdőképernyőre navigál az alkalmazásból, és hirtelen egy hirdetés jelenik meg a kezdőképernyőn.

- Olyan hirdetések, amelyek a kezdőképernyő gomb megnyomásakor, illetve a kifejezetten az alkalmazásból történő kilépéshez tervezett egyéb funkciók használatakor jelennek meg:



① A felhasználó megpróbál kilépni az alkalmazásból, hogy a kezdőképernyőre navigáljon, de a várt folyamatot megszakítja egy hirdetés.

Jobb hirdetési élmény

A fejlesztőknek meg kell felelniük a hirdetésekre vonatkozó következő irányelveknek, hogy a felhasználóknak kiváló minőségű élményt biztosíthassanak olyankor, amikor azok a Google Play

alkalmazásait használják. Hirdetéseid nem jelenhetnek meg a következő váratlan módokon a felhasználók számára:

- Nem megengedettek azok a teljes képernyős közbeiktatott hirdetések semmilyen formátumban (sem videóként, sem GIF-ként, sem statikus formátumban stb.), amelyek váratlanul jelennek meg, jellemzően olyankor, amikor a felhasználó valami más tevékenység elvégzését választja.
  - Nem megengedettek a játékmenet során a valamely szint kezdetekor vagy tartalomszegmens kezdetekor megjelenő hirdetések.
  - Nem megengedettek az alkalmazás betöltési képernyője előtt megjelenő, teljes képernyős videós közbeiktatott hirdetések.
- Nem megengedett a teljes képernyős közbeiktatott hirdetések semmilyen olyan formátuma, amely 15 másodperc elteltével nem zárható be. Azok a feliratkozást kérő, teljes képernyős közbeiktatott hirdetések, és azok, amelyek nem szakítják meg a felhasználókat a tevékenységeikben (például egy játékalkalmazás eredményképernyője után), 15 másodpercet meghaladóan is láthatók maradhatnak.

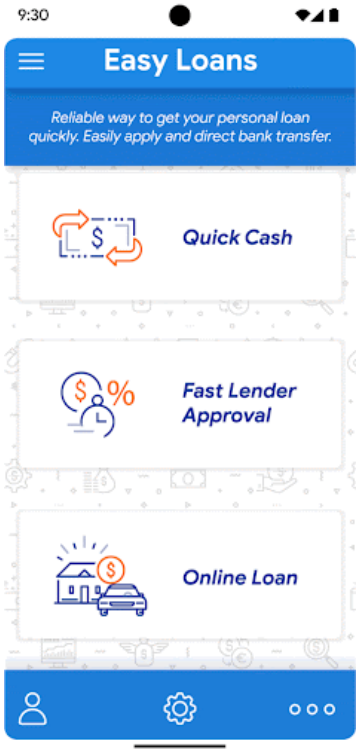
Ez az irányelv nem vonatkozik azokra a jutalommal járó hirdetésekre, amelyek megtekintésére a felhasználók kifejezetten maguk jelentkeznek (például amikor a fejlesztő kifejezetten felajánlja a felhasználónak, hogy a megtekintés fejében felold számára egy bizonyos játékfunkciót vagy tartalomrészletet). Nem vonatkozik az irányelv az olyan bevételszerzésre és hirdetésre sem, amely nem zavarja a rendes alkalmazáshasználatot vagy játékmenetet (ilyen például az integrált hirdetéseket megjelenítő videotartalom vagy a nem teljes képernyős szalaghirdetés).

Ezeket az irányelveket a Jobb hirdetések szabványa – A mobilalkalmazások biztosította élmény című irányelv inspirálta. A Jobb hirdetések szabványára vonatkozó további információval a Coalition for Better Ads szolgálhat.

Néhány példa a gyakori irányelvsértésekre:

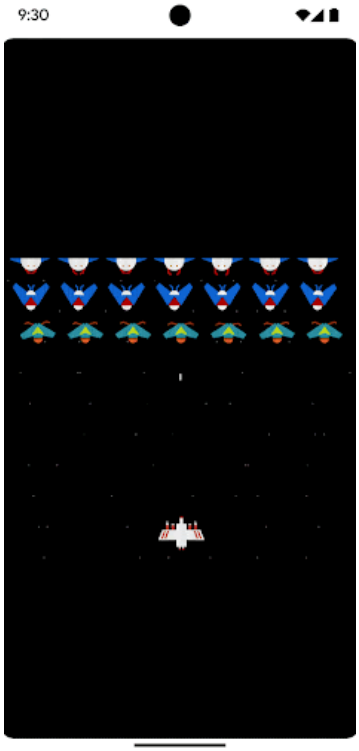
- A játékmenet során vagy egy tartalomszegmens előtt megjelenő váratlan hirdetések (például miután a felhasználó valamilyen gombra kattintott, és mielőtt a gombra való kattintás által kiváltandó művelet végrehajtódna). Ezek a hirdetések váratlanok a felhasználók számára, mivel a felhasználók a játék elkezdődésére vagy valamilyen tartalommal való műveletre számítottak helyettük.

① Váratlan statikus hirdetés jelenik meg a játékmenet során egy szint kezdetén.



② Váratlan videóhirdetés jelenik meg egy tartalomszegmens kezdetén.

- Egy teljes képernyős hirdetés, amely a játékmenet során jelenik meg, és 15 másodperc elteltével sem zárható be.



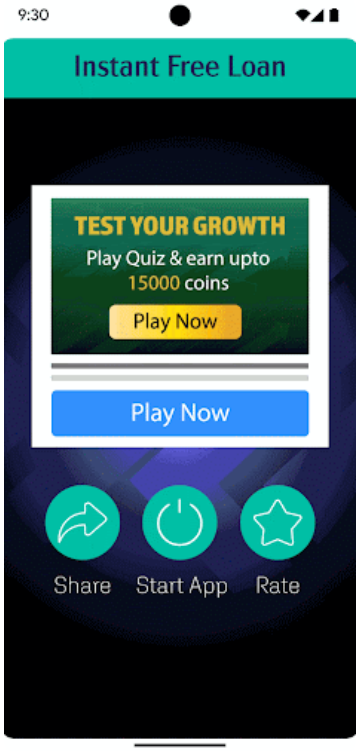
① Egy közbeiktatott hirdetés jelenik meg a játékmenet során, és nem kínálja fel a felhasználóknak 15 másodpercen belül a kihagyás lehetőségét.

Hirdetésekhez készült

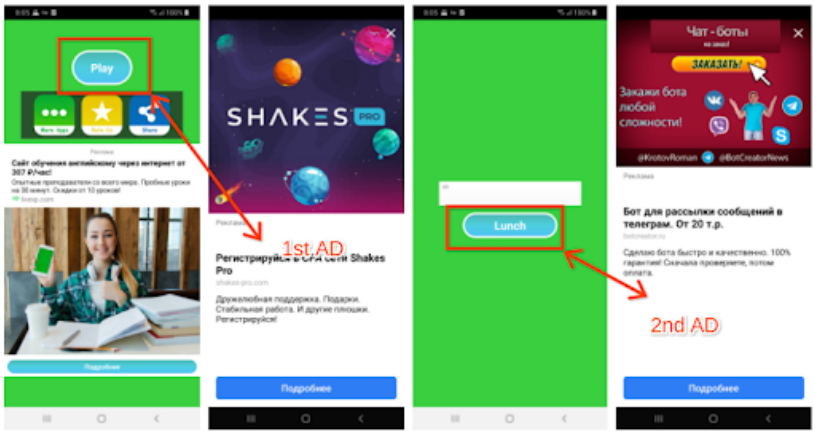
Nem engedélyezzük azokat az alkalmazásokat, amelyek közbeiktatott hirdetéseket jelenítenek meg ismétlődő módon azért, hogy így elvonják a felhasználók figyelmét az alkalmazással való interakciótól és az alkalmazáson belüli feladatok végrehajtásától.

Néhány példa a gyakori irányelvsértésekre:

- Azok az alkalmazások, amelyeknél egy közbeiktatott hirdetés van elhelyezve konszekutív módon valamilyen felhasználói művelet (beleértve, de nem kizárólagosan a kattintásokat, ujjal csúsztatásokat stb.) után.



① Az első alkalmazáson belüli oldalon több gomb is szerepel. Amikor a felhasználó az alkalmazás használatához az „**Alkalmazás indítása**” elemre kattint, egy közbeiktatott hirdetés ugrik elő. A hirdetés bezárása után a felhasználó visszatér a hirdetésre, és a **Szolgáltatás** elemre kattint a szolgáltatás használatának megkezdéséhez, de egy másik közbeiktatott hirdetés jelenik meg.



② Az első oldalon a felhasználót az **Indítás** elemre való kattintáshoz vezeti a rendszer, mivel az az alkalmazás használatához rendelkezésre álló egyetlen gomb. Amikor a felhasználó rákattint, egy közbeiktatott hirdetés jelenik meg. A hirdetés bezárása után a felhasználó az **Indítás** elemre kattint, mivel az az egyetlen gomb, amelyet használhat, és egy másik közbeiktatott hirdetés ugrik elő.

Lezárási képernyőhöz kapcsolódó bevételszerzés

Amennyiben az alkalmazásnak a kizárólagos funkciója nem a lezárási képernyő, az alkalmazások nem tartalmazhatnak olyan hirdetéseket és funkciókat, amelyek bevételt szereznek az eszköz lezárt képernyőjéből.

Hirdetési csalás

A hirdetési csalás szigorúan tilos. További információért lásd a hirdetési csalásokkal kapcsolatos irányelvünket.

Helyadatok használata hirdetésekhez

Azokra az alkalmazásokra, amelyek a jogosultságalapú eszközhelyadatok felhasználását kiterjesztik hirdetések megjelenítésére, a személyes és bizalmas adatokra vonatkozó irányelv érvényes, ezenkívül meg kell felelniük a következő követelményeknek is:

- A jogosultságalapú eszközhelyadatok hirdetési célokra való felhasználásáról vagy gyűjtéséről egyértelműen tájékoztatni kell a felhasználót, emellett ezt a tényt dokumentálni kell az alkalmazás kötelező adatvédelmi irányelveiben. Ennek a dokumentációnak tartalmaznia kell a hirdetési hálózatok vonatkozó, a helyadatok felhasználásával foglalkozó adatvédelmi irányelveire mutató linkeket is.
- A helymeghatározási jogosultságra vonatkozó követelményeknek megfelelően helymeghatározási jogosultság csak az alkalmazás meglévő funkcióinak vagy szolgáltatásainak megvalósítása céljából kérhető, kizárólag hirdetések használata céljából nem.

Az Android-hirdetésazonosító használata

A Google Play-szolgáltatások 4.0-s verziója új API-kat és azonosítót vezetett be a hirdetések és elemzések szolgáltatói számára. Az azonosító használatának feltételei alább találhatók.

- **Használat**. Az Android-hirdetésazonosító (AAID) csak hirdetési céllal és a felhasználói statisztikákhoz használható. „Az érdeklődésen alapuló hirdetések letiltása” és a „Leiratkozás a személyes hirdetésekről” beállítás állapotát az azonosító minden beolvasásakor ellenőrizni kell.
- **Személyazonosításra alkalmas adatokkal vagy más azonosítókkal való társítás**.
  - Hirdetéshasználat: A hirdetésazonosító nem kapcsolható össze állandó eszközazonosítókkal (például: SSAID, MAC-cím, IMEI stb.) hirdetési célokból. A hirdetési azonosító csak a felhasználó kifejezett beleegyezésével kapcsolható személyazonosításra alkalmas adatokhoz.
  - Elemzési használat: A hirdetési azonosító semmilyen elemzési célból nem kapcsolható személyazonosításra alkalmas adatokhoz, és nem társítható állandó eszközazonosítóval (például SSAID-vel, MAC-címmel, IMEI-vel stb.). Az állandó eszközazonosítókkal kapcsolatos további útmutatás a felhasználói adatokra vonatkozó irányelvekben található.
- **A felhasználók döntésének tiszteletben tartása**.
  - Visszaállítás esetén az új hirdetésazonosító nem kapcsolható korábbi hirdetésazonosítóhoz, sem pedig korábbi hirdetésazonosítóból származó adatokhoz a felhasználó kifejezett hozzájárulása nélkül.
  - Tiszteletben kell tartani a felhasználó „Az érdeklődésen alapuló hirdetések letiltása” és „Leiratkozás a személyes hirdetésekről” beállítását. Ha a felhasználó engedélyezte ezt a beállítást, akkor a hirdetésazonosító nem használható felhasználói profilok létrehozására hirdetési célból vagy a felhasználók személyre szabott hirdetésekkel történő célzására. Az engedélyezett tevékenységek közé tartozik a kontextuális hirdetés, a gyakoriságkorlátozás, a konverziókövetés, a jelentéskészítés, a biztonság és a csalásfelderítés.
  - Újabb eszközökön, amikor a felhasználó törli az Android-hirdetésazonosítót, a rendszer el is távolítja azt. Az azonosítóhoz való hozzáférési kísérletek nullás karakterláncot eredményeznek. A hirdetésazonosító nélküli eszközök nem kapcsolhatók korábbi hirdetésazonosítóhoz társított vagy abból származtatott adatokhoz.
- **Átláthatóság a felhasználók számára**. A hirdetésazonosító gyűjtését és használatát, valamint a jelen szerződési feltételek betartását a jogszabályoknak megfelelő adatvédelmi közleményben kell tudatni a felhasználókkal. Az adatvédelmi alapelveinkről a felhasználói adatokra vonatkozó irányelvünk nyújt további tájékoztatást.
- **Az általános szerződési feltételek betartása**. A hirdetésazonosítót csak a Google Play Fejlesztői Programszabályzatnak megfelelően szabad használni, ideértve az üzleti tevékenység részeként történő, külső felekkel való megosztást. A Google Playre feltöltött, illetve az ott közzétett valamennyi

alkalmazásnak a hirdetésazonosítót kell használnia (ha rendelkezésre áll az eszközön) minden egyéb, hirdetési céllal használt eszközazonosító helyett.

További információ a felhasználói adatokra vonatkozó irányelvekben.

Előfizetések

A fejlesztő nem vezetheti félre a felhasználókat az alkalmazásban kínált előfizetéses szolgáltatásokkal és tartalmakkal kapcsolatban. Alapvető elvárásunk, hogy az alkalmazáson belüli promóciók és a betöltési képernyők egyértelmű információkat nyújtsanak. Nem engedélyezünk olyan alkalmazásokat, amelyek megtévesztő vagy manipulatív vásárlási élményeknek teszik ki a felhasználókat (beleértve az alkalmazáson belüli vásárlásokat vagy előfizetéseket).

Az ajánlatoknak átláthatóknak kell lenniük. Ez azt jelenti, hogy a fejlesztőnek egyértelműen meg kell fogalmaznia az ajánlat feltételeit, fel kell tüntetnie az előfizetés költségét és a számlázási ciklus gyakoriságát, valamint tájékoztatnia kell a felhasználókat arról, hogy előfizetés szükséges az alkalmazás használatához. Nem szabad arra kényszeríteni a felhasználókat, hogy ezen információk áttekintéséhez további lépéseket kelljen elvégezniük.

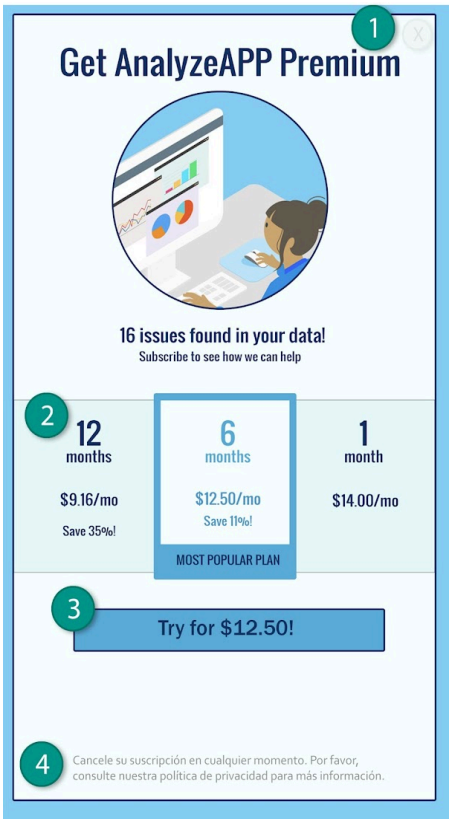
Az előfizetésnek hosszan tartó vagy ismétlődő értéket kell nyújtania a felhasználó számára az előfizetés időtartama alatt. Az előfizetés nem használható arra, hogy a fejlesztő egyszeri előnyöket kínáljon a felhasználóknak (például olyan cikkszámok, amelyek egy összegben kínálnak alkalmazáson belüli jóváírást/pénznemet vagy egyszer felhasználható, játékteljesítményt fokozó elemet). Az előfizetés ajánlhat ösztönzőket vagy promóciós bónuszokat, de ezeknek az előfizetés időtartama alatt meglévő hosszan tartó vagy ismétlődő értéket kell kiegészíteniük**.** A hosszan tartó vagy ismétlődő értéket nem ajánló termékeknek alkalmazáson belüli terméket kell használniuk az előfizetéses termék helyett.

Az egyszeri előnyöket nem állíthatod be félrevezető módon előfizetésnek a felhasználók számára. Idetartozik többek között az is, hogy nem módosíthatod az előfizetést egyszeri ajánlatra (például nem vonhatod vissza, szüntetheted meg vagy minimalizálhatod az ismétlődő értéket), miután a felhasználó megvásárolta az előfizetést.

Néhány példa a gyakori irányelvsértésekre:

- Havi előfizetések, amelyek nem tájékoztatják arról a felhasználókat, hogy az előfizetés megújítása és a fizetési eszköz terhelése automatikusan megtörténik minden hónapban.
- Éves előfizetések, amelyek a havi költséget jelenítik meg a legfeltűnőbb módon.
- Nem teljesen lokalizált előfizetési árak és feltételek.
- Alkalmazáson belüli promóciók, amelyek nem jelzik egyértelműen, hogy a felhasználó előfizetés nélkül is hozzáférhet a tartalomhoz (amennyiben ez lehetséges).
- Cikkszámnevek, amelyek nem adnak egyértelmű tájékoztatást az előfizetés jellegéről; például automatikusan ismétlődő terhelést magával vonó előfizetés esetén: „Díjmentes próbaidőszak” vagy „Próbáld ki a Prémium-tagságot – 3 napig díjmentesen”.
- Több képernyő a vásárlási folyamatban, amelyek ahhoz vezethetnek, hogy a felhasználó véletlenül az előfizetés gombra kattint.
- Olyan előfizetések, amelyek nem ajánlanak hosszan tartó vagy ismétlődő értéket: például 1000 drágakövet ajánl az első hónapban, majd az előfizetés következő hónapjaiban ez az előny 1 drágakőre csökken.
- A felhasználó kötelezése arra, hogy megvásároljon egy automatikusan megújuló előfizetést, hogy hozzájuthasson egy egyszeri előnyhöz, és a felhasználó előfizetésének törlése a vásárlás után a felhasználó megkérdezése nélkül.

1. példa:



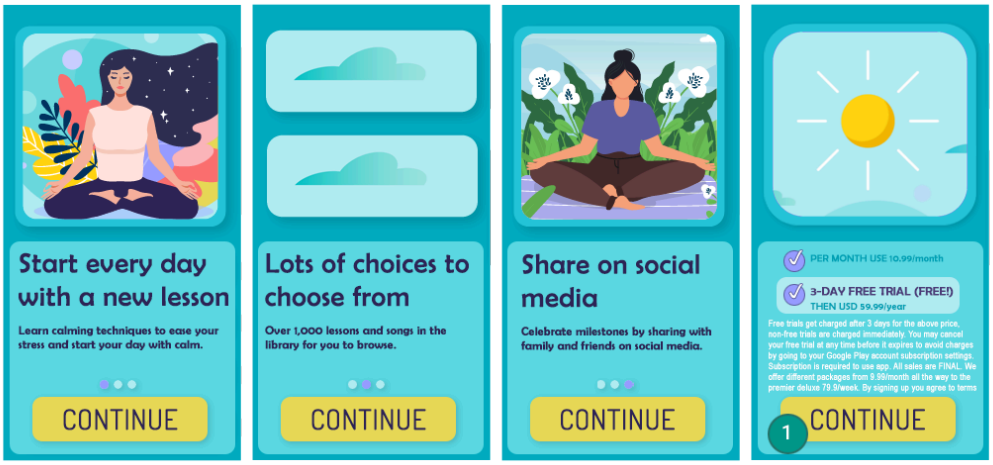
① Az elvetésre szolgáló gomb nem látható jól, ezért a felhasználók számára nem világos, hogy az előfizetési ajánlat elfogadása nélkül is hozzáférhetnek a funkciókhoz.

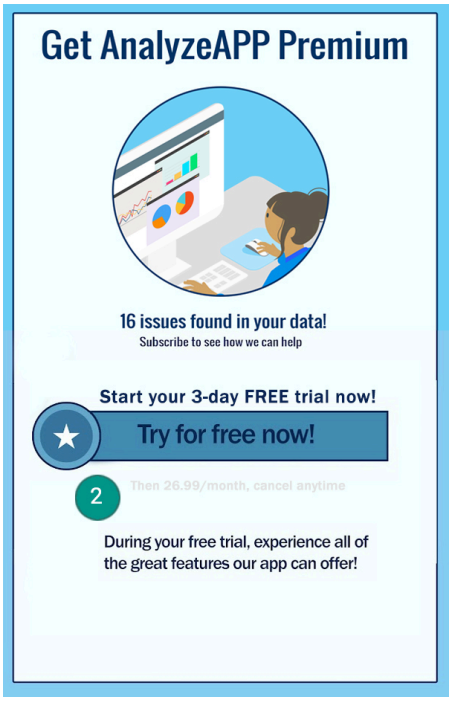
② Az ajánlat csak havi költség formájában jeleníti meg az árazást, ezért a felhasználók számára nem világos, hogy előfizetéskor hat hónapnyi díjat fizetnek ki.

③ Az ajánlat csak a bevezető árat mutatja, ezért a felhasználók számára nem világos, hogy a bevezető időszak lejártakor milyen összeget fizetnek majd automatikusan.

④ Az ajánlatot a szerződéses feltételekkel azonos nyelvre kell lokalizálni, hogy a felhasználók pontosan tájékozódhassanak az ajánlat mibenlétéről.

2. példa:





① Ismétlődő kattintások ugyanazon a gombterületen, emiatt a felhasználó véletlenül az utolsó „tovább” gombra kattintva előfizet.

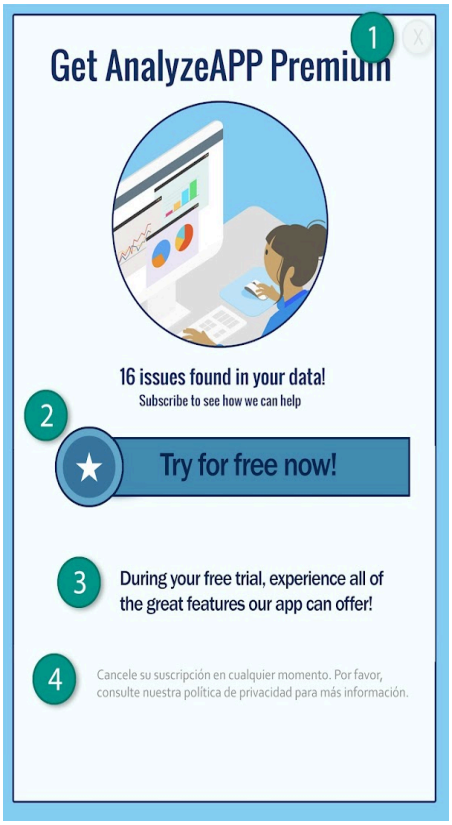
② Nehezen olvasható ki, hogy a próbaidőszak végén milyen összeggel lesz megterhelve a felhasználó számlája. A felhasználó emiatt azt hiheti, hogy a csomag díjmentes.

Díjmentes próbaidőszak és bevezető ajánlatok

Mielőtt a felhasználók előfizetnének: Önnek egyértelműen és pontosan le kell írnia az ajánlati feltételeket, beleértve a hozzáférhetővé tett tartalom vagy szolgáltatás jellegét, valamint a hozzáférés időtartamát és árát. Tájékoztatnia kell a felhasználókat arról is, hogy a díjmentes próbaidőszak hogyan és mikor vált tényleges előfizetésre, mennyibe kerül az előfizetés, és hogyan mondható le, ha a felhasználó nem szeretne váltani a próbaidőszak végén.

Néhány példa a gyakori irányelvsértésekre:

- Ajánlatok, amelyek nem árulják el egyértelműen, hogy meddig tart a díjmentes próbaidőszak vagy a bevezető ár.
- Ajánlatok, amelyek nem tájékoztatják egyértelműen arról a felhasználót, hogy az ajánlatban meghatározott időszak leteltekor előfizetése automatikusan fizetős hozzáférésre vált majd.
- Ajánlatok, amelyek nem jelzik egyértelműen, hogy a felhasználó próbaidőszak nélkül is hozzáférhet a tartalomhoz (amennyiben ez lehetséges).
- Nem teljesen lokalizált ajánlati árak és feltételek.



① Az elutasításra szolgáló gomb nem látható jól, ezért a felhasználók számára nem világos, hogy a díjmentes próbaidőszak aktiválása nélkül is hozzáférhetnek a funkciókhoz.

② Az ajánlat a díjmentes próbaidőszakot hangsúlyozza, ezért a felhasználók számára nem világos, hogy a próbaidőszak végén automatikusan elindul a tényleges előfizetés.

③ Az ajánlat nem nyújt tájékoztatást a díjmentes próbaidőszakról, ezért a felhasználók számára nem világos, hogy mennyi időre kapnak díjmentes hozzáférést az egyébként előfizetést igénylő tartalomhoz.

④ Az ajánlatot az általános szerződési feltételekkel azonos nyelvre kell lokalizálni, hogy a felhasználók pontosan tájékozódhassanak az ajánlat mibenlétéről.

Előfizetések kezelése, lemondás és visszatérítések

Ha előfizetést értékesítesz az alkalmazásodban, akkor gondoskodnod kell arról, hogy alkalmazásod egyértelműen közölje, a felhasználó miként kezelheti vagy mondhatja le az előfizetését. Alkalmazásodba az előfizetés lemondására szolgáló, egyszerűen használható, online metódushoz való hozzáférést is be kell építened. Alkalmazásod fiókbeállításaiban (vagy az annak megfelelő oldalon) az alábbiakkal teljesíthető ez a követelmény:

- a Google Play előfizetési központjára mutató link (a Google Play számlázási rendszerét használó alkalmazások esetében); és/vagy
- közvetlen hozzáférés biztosítása a lemondási folyamathoz.

Ha a felhasználó a Google Play számlázási rendszerén keresztül vásárolt előfizetést mond le, az irányelveink szerint nem kap visszatérítést az aktuális számlázási időszakra, de annak hátralévő tartama során továbbra is megkapja az előfizetésért járó tartalmat, függetlenül a lemondás dátumától. A felhasználói lemondás az aktuális számlázási időszak leteltekor lép érvénybe.

Lehetőséged van arra (a tartalom vagy a hozzáférés szolgáltatójaként), hogy rugalmasabb visszatérítési irányelveket alkalmazz. A felelősséged, hogy értesítsd a felhasználóidat az előfizetésre, az előfizetés lemondására és a visszatérítésre vonatkozó saját irányelveid esetleges változásairól, ahogyan az is, hogy az irányelvek megfeleljenek a vonatkozó jogszabályoknak.

Családbarát öntanúsító hirdetési SDK program

Ha hirdetéseket jelenítesz meg alkalmazásodban, és a célközönségedbe csak gyermekek tartoznak (a Családokkal kapcsolatos irányelvben leírtak szerint), akkor csak olyan hirdetési SDK-verziókat használhatsz, amelyek öntanúsításuk szerint megfelelnek a Google Play irányelveinek, beleértve az alább szereplő Családbarát öntanúsító hirdetési SDK-ra vonatkozó követelményeket.

Amennyiben alkalmazásod célközönségébe gyermekek és idősebbek is tartoznak, akkor gondoskodnod kell arról (például a semleges életkorszűrésre irányuló intézkedések használatával), hogy a gyermekeknek megjelenő hirdetések kizárólag az ilyen öntanúsító hirdetési SDK-verziók egyikéből érkezzenek.

A te felelősséged annak biztosítása, hogy az alkalmazásodban felhasznált valamennyi SDK-verzió – így az öntanúsító hirdetési SDK-verziók is – megfeleljen minden vonatkozó irányelvnek, helyi jogszabálynak és rendelkezésnek. A Google nem állítja és nem garantálja, hogy a hirdetési SDK-k pontos információkat közölnek az öntanúsítás során.

A családbarát öntanúsító hirdetési SDK-k használata csak akkor szükséges, ha hirdetési SDK-kat használsz a hirdetések gyermekek számára való megjelenítéséhez. Az alábbiak engedélyezettek anélkül, hogy a hirdetési SDK öntanúsítást végezne a Google Playen, de ebben az esetben is biztosítanod kell, hogy hirdetéstartalmaid és adatgyűjtési eljárásaid megfeleljenek a Google Play felhasználói adatokra vonatkozó irányelvének és a Családokkal kapcsolatos irányelvnek :

- saját hirdetések, amelyek esetében SDK-k segítségével kezeled az alkalmazásaid vagy egyéb saját tulajdonú médiatartalmaid és árucikkeid keresztpromócióját;
- közvetlen ügyletek használata a hirdetőkkel, amelyek során SDK-kat használsz a készlet kezeléséhez.

A családbarát öntanúsító hirdetési SDK-kkal kapcsolatos követelmények

- Meg kell határozni a kifogásolható hirdetéstartalmakat és viselkedéseket, és használatukat tiltani kell a hirdetési SDK általános szerződési feltételeiben vagy irányelveiben. A meghatározásoknak meg kell felelniük a Google Play Fejlesztői Programszabályzat előírásainak.
- Olyan módszert kell kialakítani, mellyel a hirdetési kreatívok korosztályok szerint besorolhatók. A korosztályokat úgy kell meghatározni, hogy legalább egy „Korhatár nélküli” és egy „Felnőtteknek” csoportot tartalmazzanak. A besorolás módszerét össze kell hangolni a Google SDK-knak biztosított módszertanával, amelyet az SDK-k az alábbi, érdeklődés kifejezésére szolgáló űrlap kitöltése után kapnak meg.
- Kérelmenkénti vagy alkalmazásonkénti alapon lehetővé kell tenni a megjelenítők számára gyermekközpontú bánásmód igénylését, amikor hirdetéseket jelenítenek meg. A bánásmódnak meg kell felelnie a vonatkozó jogszabályoknak és rendelkezéseknek, például az USA gyermekek online adatvédelmére vonatkozó törvényének (Children's Online Privacy and Protection Act; COPPA) és az EU általános adatvédelmi rendeletének (GDPR) . A gyermekközpontú bánásmód részeként a Google Play emellett megköveteli a hirdetési SDK-któl a személyre szabott hirdetések, az érdeklődésen alapuló hirdetések és a remarketing letiltását is.
- Lehetővé kell tenni a megjelenítők számára, hogy olyan hirdetésformátumokat válasszanak, amelyek megfelelnek a Google Play családokra vonatkozó hirdetési és bevételszerzési irányelveinek , valamint teljesítik a „Tanárok által jóváhagyott” program követelményeit.
- Biztosítani kell, hogy amikor a gyermekek számára való hirdetésmegjelenítés valós idejű ajánlattétel útján zajlik, megtörténjen a kreatívok ellenőrzése és az adatvédelmi jelzők továbbítása az ajánlattevők számára.
- Elegendő információt kell biztosítani (például tesztalkalmazást és az alábbi érdeklődés jelzésére szolgáló űrlapon feltüntetett adatokat) a Google számára annak igazolásához, hogy a hirdetési SDK megfelel az összes öntanúsítási követelménynek, és időben válaszolni kell a további információkérésekre, például új verziókiadásokat kell beküldeni annak igazolására, hogy a hirdetési

SDK-verzió megfelel valamennyi öntanúsítási követelménynek, illetve tesztalkalmazást kell biztosítani.
- Öntanúsítást kell végezni arról, hogy valamennyi új verziókiadás megfelel a Google Play Fejlesztői Programszabályzatnak, ideértve a Családokkal kapcsolatos irányelv követelményeit is.

Fontos: A családbarát öntanúsító hirdetési SDK-knak olyan hirdetésmegjelenítést kell támogatniuk, amely megfelel a megjelenítőkre érvényes, gyermekekkel kapcsolatos törvényeknek és jogszabályoknak.

Itt találsz további információt a hirdetési.kreatívok vízjellel való ellátásáról és tesztalkalmazás biztosításáról.

A platformok kiszolgálására vonatkozó közvetítési kérelmek a következők, amikor hirdetéseket jelenítesz meg gyerekeknek:

- csak családbarát öntanúsító hirdetési SDK-k használhatók, vagy olyan intézkedéseket kell megvalósítani, amelyekkel biztosítható, hogy a közvetítésből származó hirdetések mindegyike megfeleljen ezeknek a követelményeknek; valamint
- meg kell adni a közvetítési platformok számára szükséges adatokat a hirdetéstartalom besorolásának és a gyermekközpontú bánásmódnak a jelzésére.

A fejlesztők itt találják a családbarát öntanúsító hirdetési SDK-k listáját, és itt ellenőrizhetik, hogy a hirdetési SDK-k mely verziói tanúsították, hogy használhatók Családbarát alkalmazásokban.

Emellett a fejlesztők megoszthatják ezt az érdeklődés jelzésére szolgáló űrlapot is azon hirdetési SDK-kkal, amelyek öntanúsítást kívánnak végezni.

Áruházi adatlap és promóció

Az alkalmazáspromóció és -láthatóság nagymértékben befolyásolja az áruházbeli minőséget. Kerülje a spam jellegű áruházi adatlapokat, a gyenge minőségű promóciókat, valamint az alkalmazások Google Play-láthatóságának mesterséges javítására irányuló kísérleteket.

Alkalmazáspromóció

Nem engedélyezzük az olyan alkalmazásokat, amelyek közvetlenül vagy közvetve olyan promóciós gyakorlatokat (például hirdetéseket) folytatnak, vagy azokból hasznot húznak, amelyek megtévesztőek vagy károsak a felhasználókra vagy a fejlesztői ökoszisztémára nézve. A promóciós gyakorlat akkor minősül megtévesztőnek vagy károsnak, ha működése vagy tartalma sérti a Fejlesztői programszabályzatot.

Néhány példa a gyakori irányelvsértésekre:

- Megtévesztő hirdetések használata weboldalakon, alkalmazásokban vagy más szolgáltatásokban, beleértve a rendszerértesítésekhez és riasztásokhoz hasonló értesítéseket.
- Nyíltan szexuális jellegű hirdetések használata arra, hogy a felhasználókat az alkalmazás Google Play-adatlapjára irányítsa az alkalmazás letöltéséhez.
- Olyan promóciós vagy telepítési taktika alkalmazása, amely átirányítja a felhasználókat a Google Playre vagy egy alkalmazás letöltéséhez a felhasználó tájékoztatása nélkül.
- SMS-szolgáltatáson keresztül történő kéretlen promóció.
- Olyan szöveg vagy kép az alkalmazás címében, ikonjában vagy a fejlesztő nevében, amely utal az alkalmazás áruházi teljesítményére vagy helyezésére, árat vagy promóciós információkat tartalmaz, illetve amely az aktuális Google Play-programokkal való kapcsolatra utal.

A fejlesztő felelőssége annak biztosítása, hogy az alkalmazáshoz tartozó minden hirdetési hálózat, társult vállalkozás vagy hirdetés megfeleljen ezeknek az irányelveknek.

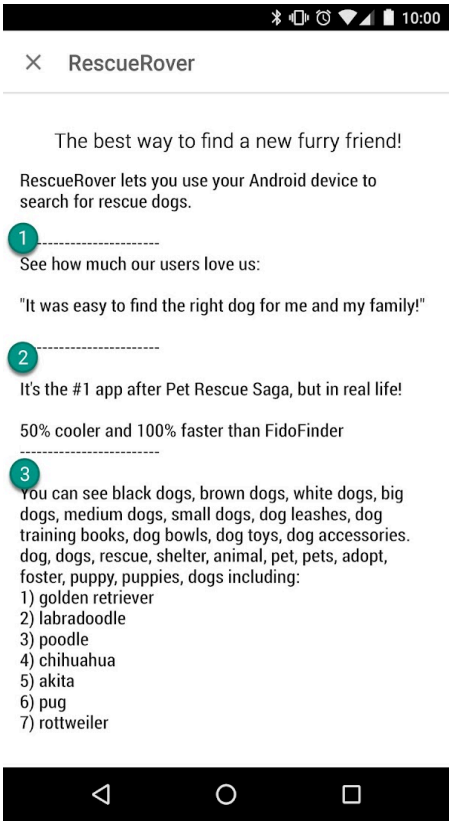
Metaadatok

A felhasználóknak szükségük van az alkalmazásod leírására ahhoz, hogy megismerjék annak funkcióját és célját. Nem engedélyezünk olyan alkalmazásokat, amelyek félrevezető, nem megfelelően formázott, nem leíró, lényegtelen, túlzó vagy kifogásolható metaadatokat tartalmaznak – többek között a fejlesztő nevére, valamint az alkalmazás leírására, címére, ikonjára, képernyőképeire és promóciós képeire vonatkozóan. A fejlesztőknek egyértelmű és jól megfogalmazott leírást kell biztosítaniuk az alkalmazáshoz. Szerző nélküli és névtelen felhasználói ajánlások sem szerepelhetnek az alkalmazás leírásában.

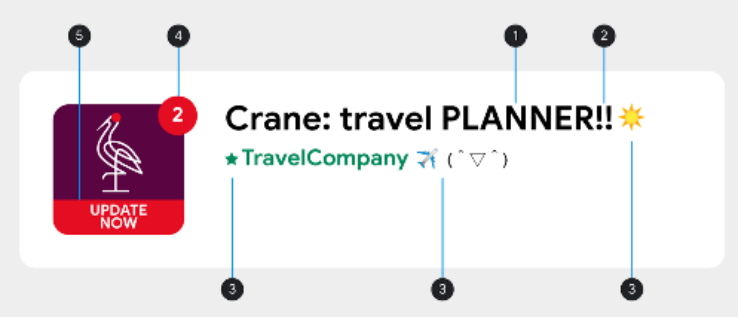
Az alkalmazás címe, ikonja és a fejlesztő neve különösen hasznos lehet a felhasználók számára az alkalmazás megtalálásához és megismeréséhez. Emojik, hangulatjelek és ismétlődő speciális karakterek nem használhatók ezekben a metaadat-elemekben. Kerülendő a CSUPA NAGYBETŰK használata, kivéve, ha ez a márkanév része. Az alkalmazásikonokban használt félrevezető szimbólumok nem engedélyezettek. Ilyen például az új üzenetre figyelmeztető pont, amikor nincs új üzenet, vagy a letöltés/telepítés szimbólum, amikor az alkalmazáshoz nem kapcsolódik tartalom letöltése. Az alkalmazás címe legfeljebb 30 karakterből állhat. Ne használj olyan szöveget vagy képet az alkalmazás címében, ikonjában vagy a fejlesztő nevében, amely utal az alkalmazás áruházi teljesítményére vagy helyezésére, árat vagy promóciós információkat tartalmaz, illetve amely az aktuális Google Play-programokkal való kapcsolatra utal.

Az itt felvázolt követelményeken felül a Google Play bizonyos fejlesztői irányelvei további metaadat-információk megadását is megkövetelhetik.

Néhány példa a gyakori irányelvsértésekre:

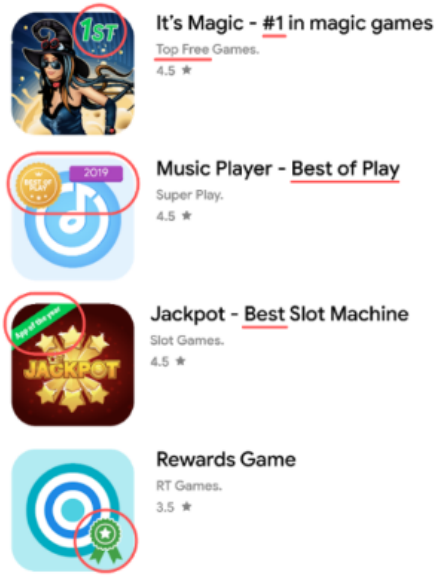


① Szerző nélküli és névtelen felhasználói ajánlások
② Alkalmazások és márkák adatainak összehasonlítása
③ Szavakból álló tömbök és szavak függőleges/vízszintes listája

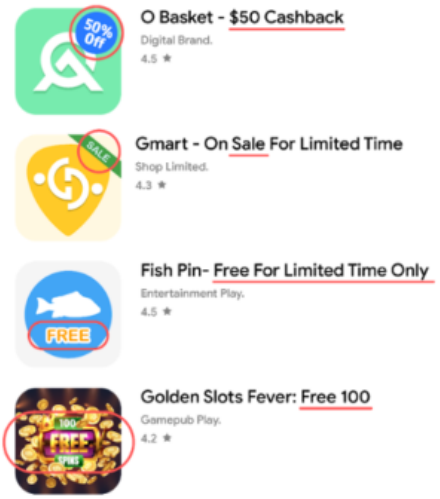


① CSUPA NAGYBETŰVEL írt szöveg, ha nem a márkanév része
② Az alkalmazás szempontjából irreleváns speciáliskarakter-sorok
③ Emojik, hangulatjelek (többek között kaomojik) és speciális karakterek használata
④ Félrevezető szimbólum
⑤ Félrevezető szöveg

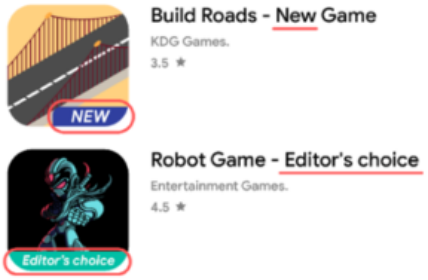
- Az áruházi teljesítményre vagy rangsorolásra utaló kép vagy szöveg (pl. „Az év alkalmazása”, „1. helyezett”, „20XX legjobbja”, „Népszerű”, díjikonok stb.)



- Árat vagy promóciós információt megjelenítő kép vagy szöveg (pl. „10% kedvezmény”, „50 USD visszajár”, „korlátozott ideig díjmentes” stb.)



- Google Play-programokra utaló kép vagy szöveg (pl. „A szerkesztő ajánlata”, „Új” stb.)



Néhány példa az adatlapon nem helyénvaló szövegekre, képekre és videókra:

- Burkolt szexuális tartalmat ábrázoló képek vagy videók. Kerülni kell a melleket, feneket, nemi szerveket vagy egyéb fetisizált testrészeket ábrázoló, burkoltan szexuális tartalmú képeket, illetve tartalmakat – legyenek azok valósak vagy ábrázoltak.
- Profán, vulgáris vagy más, a nagyközönség számára nem megfelelő nyelvezet használata az alkalmazás áruházi adatlapján.
- Nyílt erőszak szembetűnő ábrázolása az alkalmazás ikonjában, valamint a promóciós képeken és videókban.
- Tiltott droghasználat ábrázolása. Az EDSA (Educational, Documentary, Scientific, or Artistic; azaz ismeretterjesztő, oktatási, tudományos és művészeti) jellegű tartalmak áruházi adatlapjának is megfelelőnek kell lennie minden közönség számára.

Leginkább bevált módszerek:

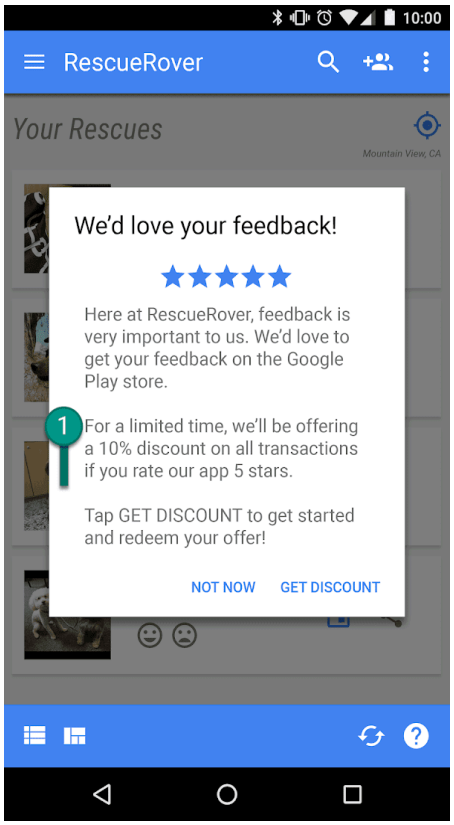
- Emeld ki az alkalmazásod előnyeit. Közölj érdekes és izgalmas tényeket az alkalmazásról, hogy a felhasználók tudják, mitől lesz különleges az alkalmazásod.
- Figyeljen arra, hogy az alkalmazás címe és leírása pontosan leírja az alkalmazás célját.
- Kerülje el az ismétlődő vagy nem odaillő kulcsszavak vagy utalások használatát.
- Az alkalmazás leírása legyen tömör és lényegre törő. A rövidebb leírások általában jobb felhasználói élményt eredményeznek, főleg a kisebb kijelzős eszközök esetében. A túl hosszú vagy részletes, nem megfelelő formátumú leírás, valamint az ismétlődés sértheti az erre vonatkozó irányelveinket.
- Ne feledje, hogy az adatlapnak mindenki számára megfelelőnek kell lennie. Kerülni kell a kifogásolható szövegek, képek és videók használatát az adatlapon, és be kell tartani a fenti irányelveket.

Felhasználói értékelések, vélemények és telepítések

A fejlesztőknek tilos megpróbálniuk befolyásolni az alkalmazások helyezését a Google Playen. Idetartozik többek között a termékértékelések, vélemények és telepítési számok szabálytalan befolyásolása, például csalárd vagy ösztönzött módszerekkel, véleményekkel és értékelésekkel, vagy ha az alkalmazás fő funkciója az, hogy a felhasználókat más alkalmazások letöltésére ösztönözze.

Néhány példa a gyakori irányelvsértésekre:

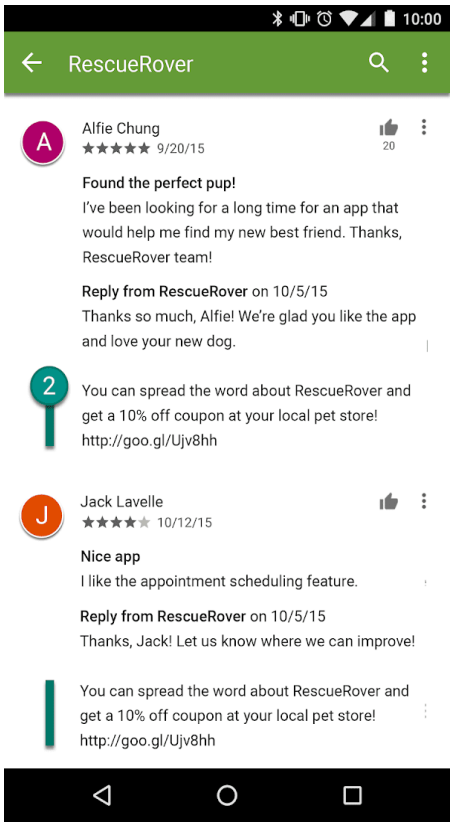
- A felhasználók megkérése, hogy valamilyen ösztönzés hatására értékeljék az alkalmazást:



① Ez az értesítés kedvezményt kínál a felhasználóknak a jó értékelésért cserébe.

- Többször is felhasználók bőrébe bújva értékelések beküldése adott alkalmazás Google Playen elfoglalt helyezésének befolyásolása céljából.

- Nem megfelelő tartalommal rendelkező vélemények beküldése, illetve a felhasználók bátorítása ennek megtételére. Nem megfelelő tartalomnak számítanak például a társalkalmazások, a kuponok, a játékbeli kódok, az e-mail-címek, valamint a webhelyekre vagy más alkalmazásokra mutató linkek:



② Ez a vélemény arra ösztönzi a felhasználókat a felajánlott kuponnal, hogy reklámozzák a RescueRover alkalmazást.

Az értékelések és vélemények az alkalmazás minőségéről tájékoztatnak. A felhasználók számítanak rá, hogy ezek hitelesek és relevánsak. Íme néhány bevált módszer a felhasználói véleményekre történő válaszadáshoz:

- Válaszában koncentráljon a felhasználó megjegyzésében felvetett problémára, és ne kérjen magasabb értékelést.
- Közöljön hasznos forrásokat (pl. támogatási e-mail-címet vagy a GYIK kapcsolódó oldalát).

Tartalombesorolások

A Google Play tartalombesorolási rendszere az International Age Ratings Coalition (Életkor Szerinti Besorolások Nemzetközi Koalíciója, IARC) besorolásait tartalmazza, és azt a célt szolgálja, hogy segítse a fejlesztőket a helyileg releváns tartalombesorolások felhasználókkal való közlésében. Azokat az irányelveket, amelyek alapján megállapítható az alkalmazás tartalmának besorolása, a regionális IARC besorolási hatóságok határozzák meg. Nem engedélyezünk olyan alkalmazásokat, amelyek nem rendelkeznek tartalombesorolással a Google Playen.

A tartalombesorolások használata

A tartalombesorolás arra szolgál, hogy tájékoztassa a fogyasztókat (elsősorban a szülőket) az alkalmazásokban megtalálható esetlegesen kifogásolható tartalmakról. Emellett segít szűrni és tiltani is a tartalmadat olyan területeken vagy bizonyos felhasználók számára, ahol a jogszabályok előírják, valamint meghatározza, hogy az alkalmazásod jogosult-e a speciális fejlesztői programokban való részvételre.

A tartalombesorolások kiosztása

Tartalombesorolás megszerzéséhez ki kell töltened az alkalmazás tartalmának jellegére vonatkozó besorolási kérdőívet a Play Console-ban . Az alkalmazás a kérdőívben megadott válaszok alapján több besorolási hatóság tartalombesorolását is megkapja. Az alkalmazás tartalmának valóstól eltérő bemutatása az alkalmazás eltávolítását, illetve felfüggesztését vonhatja maga után, ezért fontos a tartalombesorolási kérdőív pontos kitöltése.

Annak érdekében, hogy az alkalmazás ne „Nincs besorolva” megjelöléssel jelenjen meg, a Play Console-ban beküldött minden új alkalmazásodhoz, valamint a Google Playen meglévő összes alkalmazásodhoz ki kell töltened a tartalombesorolási kérdőívet. A tartalombesorolás nélküli alkalmazásokat eltávolítjuk a Play Áruházból.

Ha olyan módosításokat eszközölsz az alkalmazás tartalmára vagy funkcióira vonatkozóan, amelyek érintik a besorolási kérdőívben adott válaszokat, új tartalombesorolási kérdőívet kell beküldened a Play Console-ban.

A Súgóban további információt találhatsz a különböző besorolási hatóságokkal és azzal kapcsolatban, hogyan kell kitölteni a tartalombesorolási kérdőívet.

Besorolással kapcsolatos fellebbezések

Ha nem értesz egyet az alkalmazáshoz kapcsolt besorolással, a tanúsítványt tartalmazó e-mailben található link segítségével fellebbezhetsz közvetlenül az IARC besorolási hatóságnál.

Hírek

A híralkalmazás olyan alkalmazás, amely:

- híralkalmazásnak nyilvánítja magát a Google Play Console-on, vagy
- a „Hírek és magazinok” kategóriában tünteti fel magát a Google Play Áruházban, és a „hír” jelzővel illeti magát saját alkalmazásában, címében, ikonján, fejlesztői nevében vagy leírásában.

Példák a „Hírek és magazinok” kategóriába tartozó, híralkalmazásnak minősülő alkalmazásokra:

- Olyan alkalmazások, amelyek a „hír” jelzővel illetik magukat az alkalmazás leírásában, beleértve, de nem kizárólagosan az alábbiakat:
  - Legfrissebb hírek
  - Újság
  - Rendkívüli hírek
  - Helyi hírek
  - Napi hírek
- Olyan alkalmazások, amelyeknek alkalmazásában, címében, ikonján vagy fejlesztői nevében szerepel a „hír” szó.

Azonban ha egy alkalmazás elsősorban felhasználók által létrehozott tartalmakat tartalmaz (pl. a közösségimédia-alkalmazások), nem nyilváníthatják magukat híralkalmazásoknak, és nem is tekintendők annak.

Azon híralkalmazásoknak, amelyek esetében a felhasználónak tagságot kell vásárolnia, a vásárlás előtt előnézetet kell megjeleníteniük az alkalmazásban a tartalomról a felhasználók számára.

A híralkalmazásoknak kötelező:

- Megadniuk az alkalmazás és a cikkek tulajdonosi adatait, beleértve, de nem kizárólagosan az egyes cikkek eredeti közzétevőjét vagy szerzőjét. Abban az esetben, ha nem szokás feltüntetni az egyes cikkek szerzőit, a híralkalmazásnak kell lennie a cikkek eredeti közzétevőjének. A közösségimédia-fiókokra mutató linkeket nem tekintjük megfelelő információforrásnak a szerzőt vagy a közzétevőt illetően.
- Rendelkezniük egy olyan webhellyel vagy alkalmazáson belüli oldallal, amely egyértelműen jelzi, hogy ott találhatók a kapcsolatfelvételi adatok, és amelyet könnyű megtalálni (pl. szerepel egy rámutató link a főoldal alján vagy az oldalsó navigációs sávon), és amely tartalmazza a hírközlő szervezet érvényes kapcsolatfelvételi adatait, vagy egy e-mail-címet vagy telefonszámot. A közösségimédia-fiókokra mutató linkek nem jelentenek megfelelő kapcsolatfelvételi lehetőséget a közzétevőhöz.

A híralkalmazásoknak nem szabad:

- jelentős helyesírási és/vagy nyelvtani hibákat tartalmazniuk;
- csak statikus tartalommal rendelkezniük (pl. több hónapos tartalom); illetve
- elsődleges célként partnerprogramot vagy hirdetésekből származó bevételt megnevezniük.

Felhívjuk a figyelmedet, hogy a híralkalmazások *használhatnak* hirdetéseket és más marketinges módszereket a bevételszerzésre, ha az alkalmazás elsődleges célja nem termékek és szolgáltatások értékesítése, illetve hirdetési bevétel generálása.

A különböző megjelenítői forrásokból tartalmakat összesítő Híralkalmazásoknak egyértelműen fel kell tüntetniük a megjelenített tartalmak forrását, és minden forrásnak meg kell felelnie a Hírek szolgáltatásra vonatkozó irányelvek követelményeinek.

Ez a cikk tájékoztat arról, hogy mi a legjobb módja a szükséges adatok megadásának.

Spamek, funkciók és felhasználói élmény

Az alkalmazásoknak megfelelő szintű funkcionalitást és tartalmat kell nyújtaniuk a felhasználók számára, hogy kellemes felhasználói élményt biztosítsanak. Nem nyújtanak értéket az olyan alkalmazások, amelyek összeomlanak, a használható felhasználói élménnyel nem összeegyeztethető

egyéb viselkedést mutatnak, vagy csak az a céljuk, hogy spameljék a felhasználókat vagy a Google Playt.

Spam

Nem engedélyezzük azokat az alkalmazásokat, amelyek spamet terjesztenek a felhasználóknak vagy a Google Playen. Ide tartoznak például a felhasználóknak kéretlen üzeneteket küldő, illetve az ismétlődő, gyenge minőségű alkalmazások.

Üzenetspam

Nem engedélyezzük azokat az alkalmazásokat, amelyek a felhasználó nevében anélkül küldenek SMS-t, e-mailt vagy egyéb üzenetet, hogy lehetőséget adnának a felhasználónak a tartalom és a címzettek megerősítésére.

Példa egy gyakori irányelvsértésre:

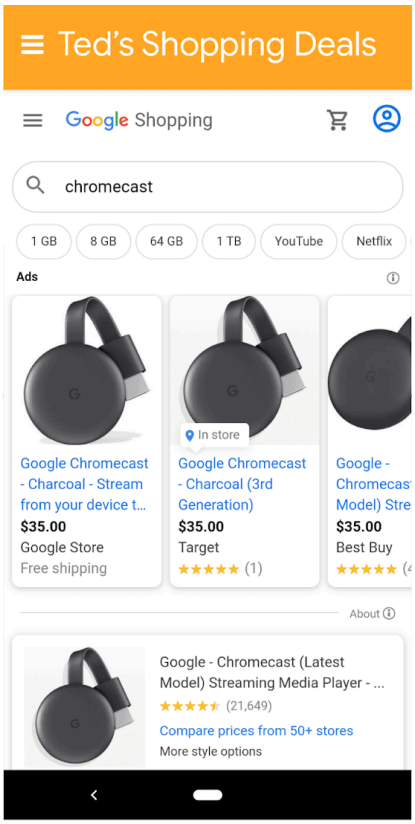
- Amikor a felhasználó megnyomja a „Megosztás” gombot, az alkalmazás üzeneteket küld a felhasználó nevében anélkül, hogy lehetőséget adna a tartalom és a címzettek megerősítésére:

Webes nézetek és partnerektől származó spam

Nem engedélyezzük azokat az alkalmazásokat, amelyek elsődleges célja a forgalom növelése valamely partneri webhelyen, illetve az érintett webhely webes nézetének megjelenítése a webhelytulajdonos vagy a rendszergazda hozzájárulása nélkül.

Néhány példa a gyakori irányelvsértésekre:

- Alkalmazás, amelynek elsődleges célja a hivatkozási forgalom növelése valamely webhelyen, hogy jóváírást kapjon az ott végrehajtott felhasználói regisztrációk vagy vásárlások után.
- Alkalmazások, amelyek elsődleges célja az, hogy engedély nélkül jelenítsék meg webhelyek webes nézetét:



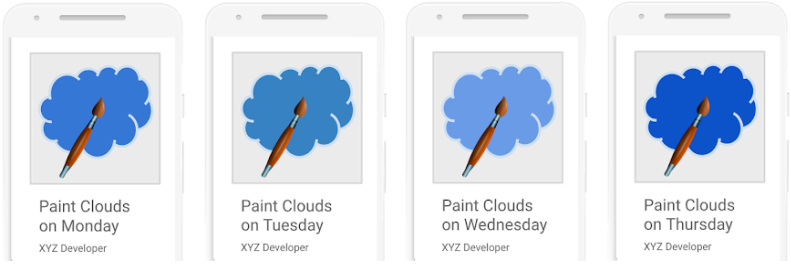
① Ennek az alkalmazásnak a neve „Ted's Shopping Deals”, de egyszerűen csak a Google Shopping webes nézetét biztosítja.

Ismétlődő tartalom

Nem engedélyezzük azokat az alkalmazásokat, amelyek mindössze ugyanazt az élményt nyújtják, mint a Google Playen már szereplő egyéb alkalmazások. Az alkalmazásoknak egyedi tartalmak vagy szolgáltatások biztosítása révén értéket kell nyújtaniuk a felhasználóknak.

Néhány példa a gyakori irányelvsértésekre:

- Tartalom más alkalmazásokból való másolása bármilyen eredeti tartalom vagy érték hozzáadása nélkül.
- Több alkalmazás létrehozása jelentős mértékben hasonló funkciókkal, tartalommal és felhasználói élménnyel. Ha ezen alkalmazások mindegyike kevés tartalommal rendelkezik, a fejlesztőknek érdemes fontolóra venni egyetlen, a teljes tartalmat összesítő alkalmazás létrehozását.



Funkció, tartalom és felhasználói élmény

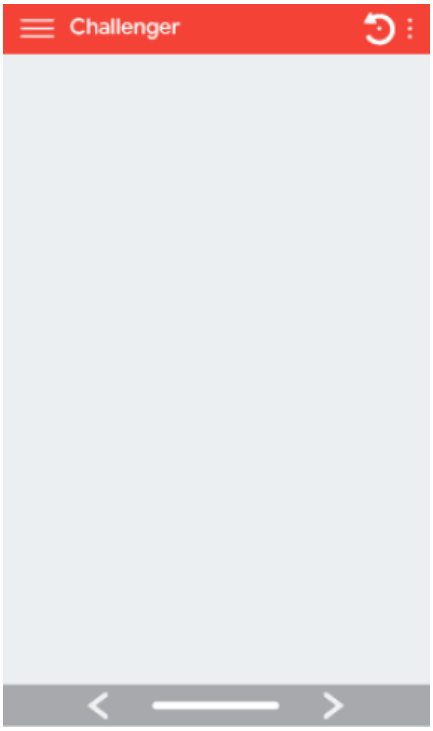
Az alkalmazásoknak stabil, reszponzív és kellemes felhasználói élményt kell nyújtaniuk. Azok az alkalmazások, amelyek összeomlanak, nem rendelkeznek a mobilalkalmazások alapvető szintű megfelelő használhatóságával, nem tartalmaznak megnyerő tartalmat, vagy más olyan viselkedést mutatnak, amely nem felel meg a funkcionális és kellemes felhasználói élménynek, nem engedélyezettek a Google Playen.

Korlátozott funkció és tartalom

Nem engedélyezünk olyan alkalmazásokat, amelyek csak korlátozott funkcionalitással és tartalommal rendelkeznek.

Példa egy gyakori irányelvsértésre:

- Statikus, alkalmazásspecifikus funkciók nélküli alkalmazások, például csak szöveges vagy PDF-fájlokat tartalmazó alkalmazások
- Nagyon kevés tartalommal rendelkező, és kellemes felhasználói élményt nem nyújtó alkalmazások, például egyszeri háttérkép alkalmazások
- Olyan alkalmazások, amelyek nem használhatók semmire, illetve nincs funkciójuk



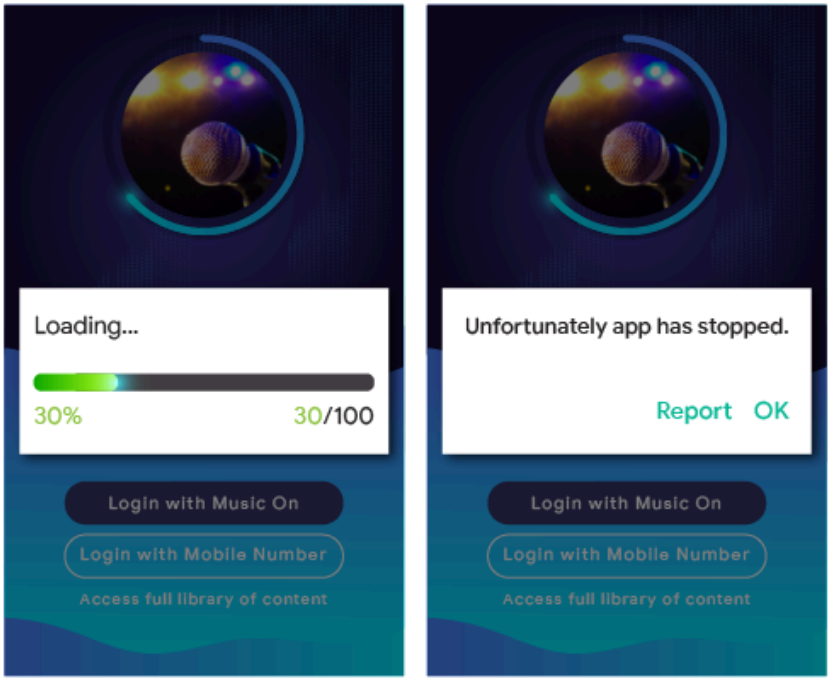
Működésképtelenség

Nem engedélyezünk olyan alkalmazásokat, amelyek összeomlanak, lefagynak, amelyeket kényszerítve lehet csak bezárni, vagy bármilyen más módon rendellenesen működnek.

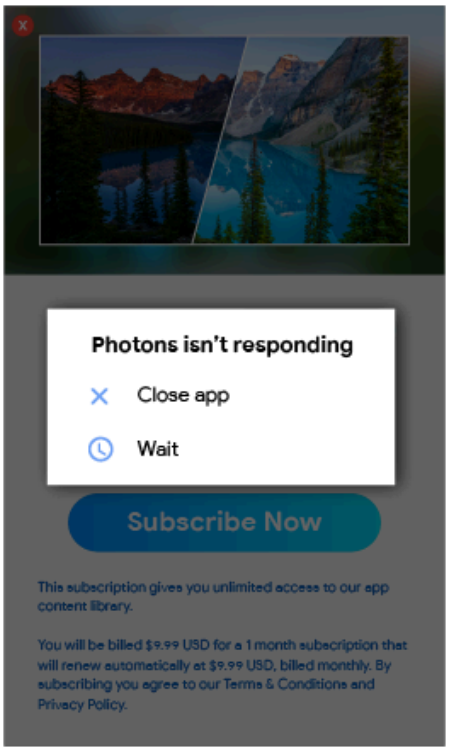
Néhány példa a gyakori irányelvsértésekre:

- **Nem települő** alkalmazások

- Települő, de **be nem töltődő** alkalmazások



- Betöltődő, de **nem reszponzív** alkalmazások



Egyéb programok

A jelen Irányelvközpont más részeiben előírt tartalmi irányelveknek való megfelelés mellett a más Android-élményekhez szánt és a Google Playen keresztül terjesztett alkalmazásoknak adott esetben a

vonatkozó programspecifikus irányelveknek is meg kell felelniük. Feltétlenül nézze át az alábbi listát, hogy megállapíthassa, vonatkozik-e valamelyik irányelv az alkalmazására.

Android Instant Apps

Az Android Instant Apps programmal az a célunk, hogy kellemes, zökkenőmentes felhasználó élményt érjünk el az adatvédelem és a biztonság legmagasabb szintű elvárásainak való megfelelés mellett. Irányelveinket úgy alakítottuk ki, hogy ezt a cél támogassák.

Azoknak a fejlesztőknek, akik a Google Playen keresztül kívánnak Android Instant Apps-alkalmazásokat terjeszteni, be kell tartaniuk az alábbi irányelveket is a Google Play Fejlesztői programszabályzata mellett.

Identitás

A fejlesztőknek integrálniuk kell a Smart Lock a jelszavakhoz funkciót a bejelentkezési funkcióval is rendelkező azonnali alkalmazásokba.

Linktámogatás

Az Android Instant Apps fejlesztői kötelesek megfelelően támogatni a más alkalmazásokra mutató linkeket. Ha a fejlesztő azonnali alkalmazásai vagy telepített alkalmazásai olyan linkeket tartalmaznak, amelyek azonnali alkalmazásra is mutathatnának, akkor a fejlesztőnek kötelessége arra az azonnali alkalmazásra irányítani a felhasználókat (például ahelyett, hogy a linkeket WebView-ban rögzítené).

Technikai előírások

A fejlesztőknek meg kell felelniük az Android Instant Appsre vonatkozóan a Google által megfogalmazott – és adott esetben módosított – technikai előírásoknak és követelményeknek, köztük a nyilvánosan hozzáférhető dokumentációinkban felsoroltaknak is.

Alkalmazástelepítés felajánlása

Az azonnali alkalmazás felajánlhat telepíthető alkalmazást, de a felajánlás nem lehet az azonnali alkalmazás elsődleges célja. Telepítés felajánlásakor a fejlesztőknek a következőkre kell figyelniük:

- A Material Design „alkalmazás letöltése” ikonját és a „telepítés” címkét kell használni a telepítés gombhoz.
- Ne legyen 2-3 implicit telepítési kérelemnél több az azonnali alkalmazásban.
- Nem szabad szalaghirdetést vagy más hirdetésszerű módot használni a telepítési kérelmek felhasználói megjelenítésénél.

További részletek és felhasználói élményre vonatkozó irányelvek az azonnali alkalmazásokkal kapcsolatban a felhasználói élmény bevált módszereivel foglalkozó oldalon találhatók.

Eszközállapot módosítása

Az azonnali alkalmazások nem módosíthatják a felhasználó eszközét az azonnali alkalmazás munkameneténél hosszabb ideig. Például nem változtathatják meg a felhasználó háttérképét, illetve nem hozhatnak létre modult a kezdőképernyőn.

Az alkalmazás láthatósága

A fejlesztőknek gondoskodniuk kell az azonnali alkalmazás láthatóságáról a felhasználó számára oly módon, hogy a felhasználó mindig tisztában legyen azzal, hogy az azonnali alkalmazás fut az eszközén.

Eszközazonosítók

Az azonnali alkalmazásoknak tilos hozzáférni az eszközazonosítókhoz, amelyekre egyszerre igaz az, hogy (1) az azonnali alkalmazás leállása után is megmaradnak, illetve hogy (2) a felhasználó nem tudja visszaállítani őket. Néhány példa (a teljesség igénye nélkül):

- Build sorozatszáma
- A hálózati chipek MAC-címei
- IMEI, IMSI

Az azonnali alkalmazások hozzáférhetnek a telefonszámhoz, ha a futási engedéllyel jutnak hozzá. A fejlesztőnek tilos kísérletet tennie arra, hogy a felhasználó azonosítási adatait ezen azonosítók használatával vagy valamilyen más módon rögzítse.

Hálózati forgalom

Az azonnali alkalmazáson belüli hálózati forgalmat TLS protokoll (például HTTPS) használatával titkosítani kell.

Az Android emojikra vonatkozó irányelve

Az emojikra vonatkozó irányelvünket úgy fogalmaztuk meg, hogy befogadó és konzisztens felhasználói élményt biztosítson. Ennek érdekében minden alkalmazásnak támogatnia kell az Unicode Emoji legfrissebb verzióját, amikor Android 12 vagy annál újabb verzión futtatják.

Azok az alkalmazások, amelyek alapértelmezés szerint Android Emojit használnak egyéni megvalósítások nélkül, már az Unicode Emoji legújabb verzióját használják, amikor Android 12 vagy annál újabb verzión futnak.

Az egyéni emojimegvalósításokkal rendelkező alkalmazásoknak, beleértve a harmadik fél könyvtár által biztosítottakat is, teljes mértékben támogatniuk kell a legfrissebb Unicode-verziót, amikor Android 12 vagy annál újabb verzión futnak, az új Unicode Emoji kiadásától számított 4 hónapon belül.

Ebből az útmutatóból megismerheted a modern emoji támogatásának módját.

Családok

A Google Play sokoldalú platformot kínál a fejlesztők számára, amelyen keresztül bemutathatják kiváló minőségű és életkor szempontjából is megfelelő tartalmaikat az egész család számára. Mielőtt a fejlesztő alkalmazást küldene be Az egész családnak programba, vagy gyermekeket célzó alkalmazást küldene be a Google Play Áruházba, köteles meggyőződni arról, hogy az alkalmazás megfelelő a gyerekek számára, és hogy megfelel az összes vonatkozó jogszabálynak.

Ismerkedjen meg a folyamattal, és tekintse át az interaktív ellenőrzőlistát az Academy for App Success oldalán.

A Google Play családokkal kapcsolatos irányelve

A családok életét tartalmasabbá tévő technológiák száma folyamatosan nő, a szülők pedig biztonságos, jó minőségű tartalmakat keresnek gyermekeik számára. Lehet, hogy a fejlesztő kifejezetten gyerekek számára készít alkalmazásokat, vagy az alkalmazása felkelti a figyelmüket. A Google Play segíteni szeretne abban, hogy a fejlesztő biztos lehessen benne: alkalmazása biztonságos minden felhasználó számára – beleértve a családokat is.

A „gyermek” szó mást és mást jelenthet a különböző nyelveken és kontextusokban. Mindenképpen ajánlott jogi tanácsot kérni arra vonatkozóan, hogy milyen kötelezettségek és korhatáros követelmények vonatkozhatnak az alkalmazásra. A fejlesztő tudja a legjobban, hogyan működik az

alkalmazása, ezért az ő segítségére hagyatkozunk, hogy biztosak lehessünk abban, hogy a Google Playen megtalálható alkalmazások biztonságosak a családok számára.

A Google Play Családokkal kapcsolatos irányelvének megfelelő összes alkalmazás jogosult a „Tanárok által jóváhagyott" programba való besorolásra, de nem tudjuk garantálni, hogy az alkalmazásod bekerül a „Tanárok által jóváhagyott" programba.

Play Console-követelmények

Célközönség és tartalom

A Google Play Console Célközönség és tartalom szakaszában még a közzététel előtt meg kell adni az alkalmazás célközönségét úgy, hogy ki kell választani a megfelelő korosztályt a listából. Függetlenül attól, hogy a fejlesztő mit ad meg a Google Play Console felületén, ha olyan képeket és szavakat használ az alkalmazásban, amelyet gyermekeknek szólóként lehet értelmezni, akkor a Google Play esetleg máshogy értékelheti az alkalmazás célközönségét. A Google Play fenntartja a jogot arra, hogy felülvizsgálja a megadott alkalmazásinformációkat, meggyőződve arról, hogy a célközönség pontosan lett meghatározva.

A fejlesztő csak akkor válasszon ki egynél több korosztályt alkalmazása célközönségeként, ha alkalmazását úgy tervezte meg – és erről meg is bizonyosodott –, hogy az alkalmazás megfelelő legyen a kiválasztott korosztályokban lévő felhasználók számára. Például a csecsemők, illetve a bölcsődés- és óvodáskorú gyermekek számára tervezett alkalmazásoknál csak a „Legfeljebb 5 évesek" lehetőséget kell kiválasztani célcsoportként. Ha alkalmazását egy konkrét iskolai képzési forma általi használatra szánja, válassza ki az annak leginkább megfelelő korosztályt. Csak akkor válasszon felnőtteket és gyerekeket is tartalmazó korosztályokat, ha alkalmazása valóban minden korosztálynak szól.

A Célközönség és tartalom szakasz frissítése

A fejlesztő bármikor frissítheti az alkalmazásinformációkat a Google Play Console Célközönség és tartalom szakaszában. Ahhoz, hogy az új információk a Google Play Áruházban is megjelenjenek, frissítenie kell az alkalmazást . A Google Play Console e szakaszában végzett módosítások irányelveknek való megfelelőségének ellenőrzésére azonban még az alkalmazásfrissítés beküldése előtt sor kerülhet.

Határozottan javasoljuk, hogy a fejlesztő az alkalmazás áruházi adatlapjának „Újdonságok" részében vagy alkalmazáson belüli értesítéseken keresztül tájékoztassa meglévő felhasználóit arról, hogy módosítani szeretné a megcélzott korosztályt, elkezdene hirdetéseket használni, vagy megvalósítana alkalmazáson belüli vásárlásokat.

Megtévesztés a Play Console-ban

Az alkalmazás Play Console-ban szereplő adatainak – beleértve a Célközönség és tartalom szakaszt – valóstól eltérő bemutatása az alkalmazás eltávolítását, illetve felfüggesztését vonhatja maga után, ezért fontos a pontos információk megadása.

Családokkal kapcsolatos irányelvekre vonatkozó követelmények

Ha az alkalmazás egyik célközönségét a gyermekek jelentik, be kell tartani a következő követelményeket. A követelmények be nem tartása az alkalmazás eltávolítását vagy felfüggesztését eredményezheti.

1. **Alkalmazástartalom**: Gyermekek számára megfelelőnek kell lennie az alkalmazás azon tartalmainak, melyek gyermekek számára hozzáférhetők. Ha az alkalmazásodban van globálisan nem helyénvaló tartalom, ami azonban gyermekkorú felhasználók számára megfelelőnek számít egy konkrét régióban, akkor az alkalmazás elérhető lehet abban az adott régióban (korlátozott régiók), de a többi régióban nem.
2. **Az alkalmazás működése:** Az alkalmazásnak nem csupán webes nézetet kell nyújtania valamely webhelyről, és nem csak valamely webhely partneri forgalmának növelése az elsődleges célja, az

adott webhelytulajdonos vagy -adminisztrátor engedélye nélkül.

3. **Válaszok a Play Console felületén:** Pontosan meg kell válaszolni az alkalmazásra vonatkozó minden kérdést a Play Console felületén, és a válaszokat az alkalmazás esetleges változásainak megfelelően frissíteni kell. Idetartozik többek között az, hogy pontos válaszokat kell adnod az alkalmazásodról a Célközönség és tartalom szakaszban, az Adatbiztonság szakaszban és az IARC tartalombesorolási kérdőívében.
4. **Adatkezelési gyakorlat**: Ha az alkalmazás gyermekekre vonatkozó személyes és bizalmas információkat gyűjt, erről tájékoztatást kell nyújtani akkor is, ha az adatgyűjtés az alkalmazás által használt vagy meghívott API-kon vagy SDK-kon keresztül történik. Gyermekekre vonatkozó bizalmas információk többek között a hitelesítési adatok, a mikrofonból és a kamerából származó adatok, az eszközadatok, az Android-azonosító és a hirdetéshasználati adatok. Biztosítani kell azt is, hogy az alkalmazás megfeleljen az alábbi adatkezelési gyakorlatoknak:
   - A kizárólag gyermekeket célzó alkalmazások nem továbbíthatnak Android-hirdetésazonosítót (AAID), SIM-sorozatszámot, buildsorozatszámot, BSSID-t, MAC-címet SSID-t, IMEI-t és/vagy IMSI-t.
     - A kizárólag gyermekeket célzó alkalmazások nem kérhetik az AD_ID engedélyt a 33-mas vagy újabb Android API célzása esetén.
   - Az olyan alkalmazások, amelyek célközönségébe gyermekek és idősebb korosztályok is tartoznak, nem továbbíthatnak a gyermektől vagy az ismeretlen korú felhasználótól Android-hirdetésazonosítót (AAID), SIM-sorozatszámot, buildsorozatszámot, BSSID-t, MAC-címet, SSID-t, IMEI-t és/vagy IMSI-t.
   - Tilos lekérni az eszköz telefonszámát az Android API TelephonyManager osztályából.
   - A kizárólag gyermekeket célzó alkalmazások nem kérhetnek helymeghatározási jogosultságot, illetve nem gyűjthetnek, nem használhatnak és nem továbbíthatnak pontos helyadatokat.
   - Az alkalmazásoknak a Companion Device Manager (CDM) szolgáltatást kell használniuk a Bluetooth-hozzáférés kéréséhez, kivéve, ha az alkalmazás kizárólag olyan operációsrendszer-verziókat céloz, amelyek nem kompatibilisek a CDM-mel.
5. **API-k és SDK-k**: Biztosítania kell az alkalmazása által használt összes API és SDK megfelelő implementálását.
   - A kizárólag gyermekeket célzó alkalmazások nem tartalmazhatnak olyan API-kat vagy SDK-kat, amelyek nem használhatók elsődlegesen gyermekeknek szóló szolgáltatásokban.
     - Idetartoznak például az olyan API-szolgáltatások, amelyek OAuth technológia segítségével végeznek hitelesítést és ellenőrzést, és amelyeknek az általános szerződési feltételeiben szerepel, hogy nem jóváhagyottak a gyermekeknek szóló szolgáltatásokban való használatra.
   - A gyermekeket és idősebbeket egyaránt célzó alkalmazások csak abban az esetben használhatnak gyermekeknek készült szolgáltatásokhoz nem jóváhagyott API-kat és SDK-kat, ha ezek csak semleges életkorszűrés után állnak rendelkezésre, vagy ha úgy implementálják őket, hogy nem gyűjtenek adatokat a gyermekekről. Az olyan alkalmazások, amelyek célközönségébe gyermekek és idősebb korosztályok is tartoznak, nem tehetik kötelezővé, hogy a felhasználók olyan API-n vagy SDK-n keresztül férhessenek hozzá az alkalmazás tartalmához, amely nincs jóváhagyva gyermekeknek készült szolgáltatásokban való használatra.
6. **Kiterjesztett valóság (AR):** Ha az alkalmazás kiterjesztett valóságot használ, biztonsági figyelmeztetést kell megjeleníteni közvetlenül a kiterjesztett valóságot tartalmazó rész elindítása előtt. A figyelmeztetésnek a következőket kell tartalmaznia:
   - megfelelő üzenetet a szülői felügyelet fontosságáról;
   - emlékeztetőt a valós világ fizikai veszélyeiről (például: figyelj a környezetedre).
   - Az alkalmazás nem követelheti meg olyan eszköz alkalmazását, amelynek használatát gyermekek számára nem javasolják (ilyen például a Daydream és az Oculus).
7. **Közösségi alkalmazások és funkciók:** Ha az alkalmazás használatával a felhasználók információkat oszthatnak meg vagy cserélhetnek, akkor pontosan közölni kell ezeket a funkciókat a Play Console tartalombesorolási kérdőívén.

- Közösségi alkalmazások: A közösségi alkalmazás olyan alkalmazás, amelynek az a fő célja, hogy lehetővé tegye a felhasználók számára adatok szabad formájú megosztását vagy személyek nagyobb csoportjával való kommunikációt. Minden olyan közösségi alkalmazásnak, amely célközönségébe a gyermekek is beletartoznak, alkalmazáson belüli emlékeztetőt kell megjelenítenie a biztonságos online jelenlétről és az online interakciók való életben jelentett kockázatairól, mielőtt megengedné, hogy a gyermekkorú felhasználók szabad formájú médiatartalmakat vagy információkat osszanak meg. Felnőtt által elvégzett műveletet is kötelezővé kell tenni, mielőtt az alkalmazás megengedné a gyermekkorú felhasználóknak a személyes adatok megosztását.
- Közösségi funkciók: Közösségi funkció minden olyan további alkalmazásfunkció, amely segítségével a felhasználók tartalmakat oszthatnak meg szabad formában, vagy személyek nagyobb csoportjával kommunikálhatnak. Minden olyan alkalmazásnak, amely célközönségébe a gyermekek is beletartoznak, és közösségi funkciókkal rendelkezik, alkalmazáson belüli emlékeztetőt kell megjelenítenie a biztonságos online jelenlétről és az online interakciók való életben jelentett kockázatairól, mielőtt megengedné, hogy a gyermekkorú felhasználók szabad formájú médiatartalmakat vagy információkat osszanak meg. Továbbá lehetőséget kell biztosítani arra, hogy a felnőttek kezelhessék a gyermekkorú felhasználók közösségi funkcióit, beleértve, de nem kizárólagosan a közösségi funkció engedélyezését/letiltását, vagy különböző funkcionalitási szintek kiválasztását. Végül kötelezővé kell tenni egy felnőtt által elvégzett műveletet azon funkciók engedélyezése előtt, amelyek segítségével a gyermekek személyes adatokat tudnak megosztani.
- A felnőtt által elvégzett művelet olyan mechanizmust jelent, amely megerősíti, hogy a felhasználó nem gyermekkorú, illetve nem ösztönzi a gyermekeket hamis életkor közlésére ahhoz, hogy az alkalmazás felnőttek részére megtervezett területeihez is hozzáférjenek (pl. felnőtt PIN-kódja, jelszó, születési dátum, e-mail-cím igazolása, fotóazonosító, bankkártya vagy TB-szám).
- Azok a közösségi alkalmazások, amelyek az ismeretlen személyekkel való csevegésre helyezik a hangsúlyt, nem célozhatnak meg gyermekeket. Példák: chatrulett-típusú alkalmazások, társkereső alkalmazások, gyermekeknek szánt nyílt csevegőszobák stb.

8. **Jogi megfelelőség:** Gondoskodni kell arról, hogy az alkalmazás és az alkalmazás által használt vagy meghívott API-k és SDK-k is megfeleljenek az USA COPPA-törvényének (Children's Online Privacy and Protection Act) és az EU általános adatvédelmi rendeletének (GDPR) , valamint minden egyéb vonatkozó törvénynek és jogszabálynak.

Néhány példa a gyakori irányelvsértésekre:

- Alkalmazások, amelyek gyerekeknek szóló játékot hirdetnek az áruházi adatlapjukon, de tartalmuk csak felnőttek számára megfelelő.
- Alkalmazások, amelyek API-jainak általános szerződési feltételei tiltják a gyermekeknek készült játékokban való felhasználást.
- Alkalmazások, amelyek alkohol, dohánytermék vagy ellenőrzött szerek használatát népszerűsítik.
- Alkalmazások, amelyek igazi vagy szimulált szerencsejátékot tartalmaznak.
- Gyermekek számára nem megfelelő, erőszakot, vérengzést és sokkoló tartalmakat magukban foglaló alkalmazások.
- Társkereső szolgáltatásokat vagy szexuális és párkapcsolati tanácsadást kínáló alkalmazások.
- Alkalmazások, amelyekben olyan webhelyekre mutató linkek találhatók, amelyek tartalma sérti a Google Play Fejlesztői programszabályzatát .
- Alkalmazások, amelyek felnőtteknek szóló hirdetéseket (pl. erőszakos tartalmat, szexuális tartalmat, szerencsejátékkal kapcsolatos tartalmat) jelenítenek meg gyermekeknek.

Hirdetések és bevételszerzés

Ha olyan alkalmazásból történik a bevételszerzés a Playen, amely gyermekeket céloz, fontos, hogy az alkalmazás kövesse a Családokra vonatkozó hirdetésekkel kapcsolatos és bevételszerzési irányelveket.

Az alábbi irányelvek érvényesek minden bevételszerzésre és hirdetésre az alkalmazásban, beleértve a hirdetéseket, keresztpromóciókat (a saját alkalmazások és harmadik féltől származó alkalmazások tekintetében), alkalmazáson belüli vásárlási ajánlatokat és minden más kereskedelmi tartalmat (mint például a fizetett termékmegjelenítést). Az ilyen alkalmazásokban lévő minden bevételszerzésnek és hirdetésnek meg kell felelnie a vonatkozó törvényeknek és jogszabályoknak (beleértve minden releváns önszabályozó és ágazati irányelvet).

A Google Play fenntartja a jogot arra, hogy elutasítsa, eltávolítsa vagy felfüggessze a túl agresszív kereskedelmi gyakorlatot folytató alkalmazásokat.

Hirdetésekre vonatkozó követelmények

Ha az alkalmazás gyermekeknek vagy ismeretlen korú felhasználóknak jelenít meg hirdetéseket, akkor:

- csak a Google Play családbarát öntanúsított hirdetési SDK használata engedélyezett az e felhasználók számára történő hirdetésmegjelenítéshez;
- meg kell győződni arról, hogy az e felhasználók számára megjelenő hirdetések nem használnak érdeklődésen alapuló hirdetést (olyan egyéni felhasználókra célzott hirdetés, akik bizonyos jellemzőkkel rendelkeznek online böngészési viselkedési szokásaik alapján) vagy remarketinget (egyéni felhasználókra célzott hirdetés az alkalmazással vagy webhellyel kapcsolatos korábbi interakciók alapján);
- meg kell győződni arról, hogy az e felhasználók számára megjelenő hirdetések tartalma megfelelő a gyermekek számára;
- meg kell győződni arról, hogy az e felhasználók számára megjelenő hirdetések betartják a családi hirdetések formátumára vonatkozó követelményeket; és
- gondoskodni kell a gyermekeknek szóló hirdetésekre vonatkozó jogszabályoknak és ipari szabványoknak való megfelelőségről.

Hirdetésformátumra vonatkozó követelmények

Az alkalmazás bevételszerzési módjai és hirdetései nem tartalmazhatnak félrevezető tartalmat, és nem szabad őket úgy megtervezni, hogy gyermekkorú felhasználók véletlenül rájuk kattintsanak.

Ha az alkalmazás kizárólagos célközönségét a gyermekek jelentik, a következőkben felsoroltak mindegyike tilos. Ha az alkalmazás célközönségét gyermekek és idősebb korúak alkotják, akkor a hirdetések gyermekek vagy ismeretlen korú felhasználók részére való megjelenítése esetén a következők mindegyike tilos:

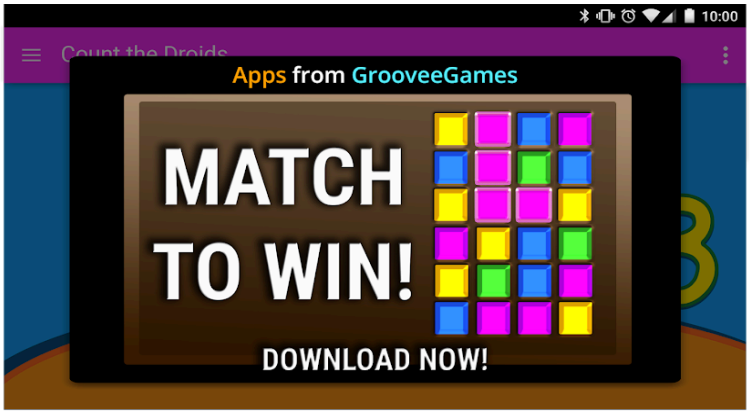
- zavaró bevételszerzési módok és hirdetések, ideértve azokat a bevételszerzési módokat és hirdetéseket, amelyek az egész képernyőt elfoglalják, vagy zavarják az alkalmazás normális használatát, és nem egyértelmű, hogy miként kell elvetni őket (ilyen például a Hirdetésfal);
- olyan bevételszerzési módok és hirdetések (így például a jutalommal járó és a feliratkozást igénylő hirdetések is), amelyek megzavarják az alkalmazás szokásos használatát vagy a játékmenetet, és nem zárhatók be 5 másodperc után;
- olyan bevételszerzési módok és hirdetések 5 másodpercnél hosszabb ideig is megjelenhetnek, amelyek nem zavarják meg az alkalmazás szokásos használatát vagy a játékmenetet (például videótartalom integrált hirdetésekkel);
- közbeiktatott bevételszerzési módok és hirdetések, amelyek az alkalmazás elindulásakor azonnal megjelennek;
- több hirdetéselhelyezés egy oldalon (nem engedélyezett például több szalaghirdetés vagy videóhirdetés megjelenítése, sem olyan szalaghirdetésé, amely több ajánlatot jelenít meg egyetlen elhelyezésen);
- az alkalmazás tartalmától nehezen megkülönböztethető bevételszerzési módok és hirdetések, például offerwall és egyéb, képernyőn maradó hirdetési élmény;
- megrázó vagy érzelmi manipulációt alkalmazó trükkök, amelyek hirdetésmegtekintést vagy alkalmazáson belüli vásárlást ösztönöznek;

- olyan megtévesztő hirdetések, amelyek átkattintásra kényszerítik a felhasználókat egy másik hirdetést aktiváló Elvetés gombbal, vagy úgy, hogy hirtelen hirdetést jelenítenek meg az alkalmazás olyan részén, ahová a felhasználó általában valamelyik másik funkció miatt koppint;
- a játékbeli virtuális pénz és az alkalmazáson belüli vásárlásokra használható valódi pénz közti különbségtétel hiánya.

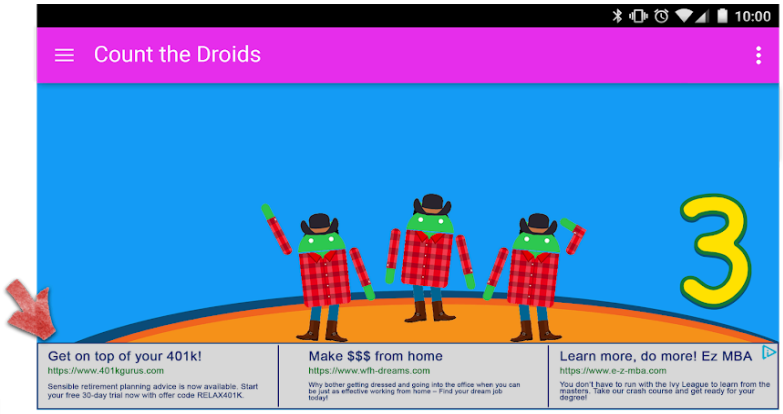
Néhány példa a gyakori irányelvsértésekre:

- Olyan bevételszerzési mód és hirdetés, amely helyet változtat, amikor a felhasználó megpróbálja bezárni
- Olyan bevételszerzési mód és hirdetés, amely nem ad lehetőséget a felhasználónak kilépni az ajánlatból öt (5) másodperc elteltével, ahogyan az alábbi példán látható:

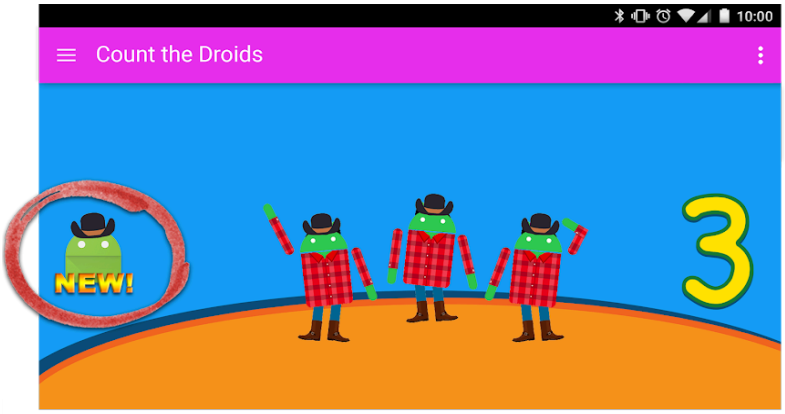
- Olyan bevételszerzési mód és hirdetés, amely a képernyő nagy részét vagy egészét betölti anélkül, hogy a felhasználó számára egyértelmű módon bezárható lenne, ahogyan az alábbi példán látható:



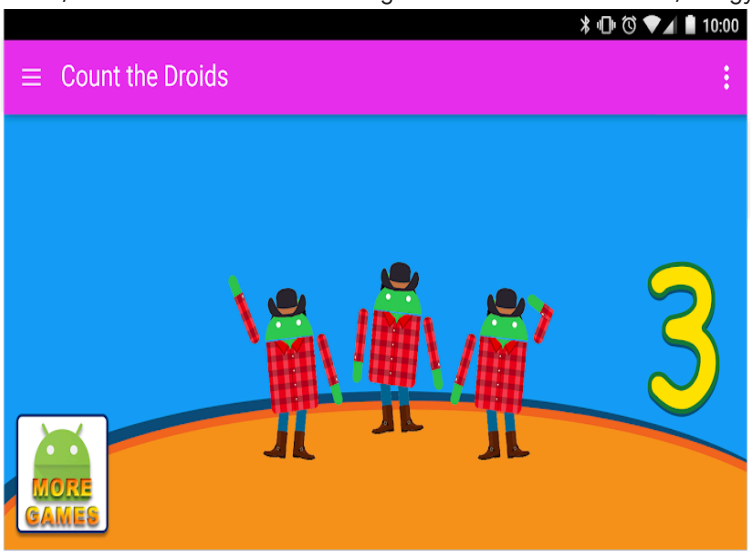
- Egyszerre több ajánlatot mutató szalaghirdetés, ahogyan az alábbi példán látható:



- Az alkalmazástartalmakkal összetéveszthető bevételszerzési mód és hirdetés, ahogyan az alábbi példán látható:



- Olyan gomb, hirdetés, vagy bevételszerzési mód, amely a fejlesztő másik Google Play áruházi adatlapját hirdeti, de nem különböztethető meg az alkalmazás tartalmától, ahogyan az alábbi példán látható:



Néhány példa a nem megfelelő, gyermekeknek nem megjeleníthető hirdetéstartalmakra.

- **Nem megfelelő médiatartalom**: Gyermekek számára nem megfelelő tévéműsorokat, mozifilmeket, zenei albumokat vagy egyéb médiatartalmat népszerűsítő hirdetések.
- **Nem megfelelő videojátékok és letölthető szoftverek**: Gyermekek számára nem megfelelő letölthető szoftvereket és videojátékokat népszerűsítő hirdetések.

- **Szabályozás alá eső és káros szerek**: Alkoholt, dohányterméket, szabályozás alá eső vagy bármilyen más káros szert népszerűsítő hirdetések.
- **Szerencsejáték**: Szimulált szerencsejátékot, sorsolást vagy nyereményjátékot népszerűsítő hirdetések, még ingyenes részvétel esetén is.
- **Felnőtteknek szóló és szexuális jellegű tartalom**: Szexualitást, burkolt szexualitást és felnőtt tartalmakat ábrázoló hirdetések.
- **Társkeresés és párkapcsolatok**: Társkereső vagy felnőtt kapcsolatokat elősegítő webhelyek hirdetései.
- **Erőszakos tartalom**: Gyermekek számára nem megfelelő erőszakos és megrázó tartalmú hirdetések.

Hirdetési SDK-k

Ha hirdetéseket jelenítesz meg alkalmazásodban, és a célközönség csak gyermekekből áll, akkor kizárólag családbarát öntanúsító hirdetési SDK-verziókat használhatsz. Amennyiben az alkalmazás célközönségébe a gyermekek és az idősebbek is beletartoznak, életkorszűrési módszereket kell alkalmazni (például semleges életkorszűrést), és biztosítani kell, hogy a gyermekeknek megjelenő hirdetések kizárólag a Google Play öntanúsító hirdetési SDK-verziókból érkezzenek.

Ezekkel a követelményekkel kapcsolatos további információt a Családbarát öntanúsító hirdetési SDK program irányelveinek oldalán találsz, a Családbarát öntanúsító hirdetési SDK-verziók aktuális listáját pedig lásd itt .

Ha az AdMob szolgáltatást használja, az AdMob Súgóban tájékozódhat a termékekkel kapcsolatban.

A te felelősséged annak biztosítása, hogy az alkalmazás megfeleljen a hirdetésekre, az alkalmazáson belüli vásárlásokra és a kereskedelmi tartalmakra vonatkozó összes követelménynek. A hirdetési SDK-k tartalmi irányelveivel és hirdetési gyakorlatával kapcsolatban az adott hirdetési hálózatnál lehet érdeklődni.

Családbarát öntanúsító hirdetési SDK-ra vonatkozó irányelv

A Google elkötelezett aziránt, hogy biztonságos élményt biztosítson a gyermekek és családok számára. A legfontosabb része ennek az elköteleződésnek annak biztosítása, hogy a gyermekek csak a koruknak megfelelő hirdetéseket láthassanak, és hogy az adataikat megfelelő módon kezeljék. E cél érdekében kötelezővé tettük a hirdetési SDK-k és közvetítési platformok számára annak az öntanúsítását, hogy gyermekek számára megfelelőek, illetve megfelelnek a Google Play Fejlesztői Programszabályzatának és a Google Play családokkal kapcsolatos irányelveinek , beleértve a Családbarát öntanúsító hirdetési SDK program követelményeit .

A Google Play Családbarát öntanúsító hirdetési SDK program segítségével a fejlesztők azonosíthatják, hogy mely hirdetési SDK-k és közvetítési platformok tanúsították önmagukról, hogy megfelelőek gyermekeknek készített alkalmazásokban való használatra.

Az SDK adatainak a valóstól eltérő bemutatása – már az érdeklődés jelzésére szolgáló űrlapon is – ahhoz vezethet, hogy eltávolítjuk az SDK-dat a Családbarát öntanúsító hirdetési SDK programból, vagy felfüggesztjük a programban való részvételét, ezért fontos a pontos információk megadása.

Irányelvi követelmények

Ha az SDK-d vagy közvetítési platformod a Google Play Családbarát programban részt vevő alkalmazásokban jelenít meg hirdetéseket, meg kell felelned a Google Play fejlesztői irányelveinek, beleértve a következő követelményeket. Ha nem tartod be a követelményeket, eltávolíthatunk a Családbarát öntanúsító hirdetési SDK programból, vagy felfüggeszthetjük a részvételed.

Te felelsz annak biztosításáért, hogy az SDK-d vagy közvetítési platformod megfeleljen az irányelveknek, ezért tekintsd át alaposan a Google Play Fejlesztői Programszabályzatát, a Google Play

Családokkal kapcsolatos irányelveit és a Családbarát öntanúsító hirdetési SDK program követelményeit.

1. **Hirdetések tartalma:** A gyermekek által hozzáférhető hirdetések tartalmainak a gyermekek számára megfelelőnek kell lenniük.
   - (i) Meg kell határoznod a kifogásolható hirdetéstartalmakat és viselkedéseket, valamint (ii) tiltanod kell őket az általános szerződési feltételeidben vagy irányelveidben. A meghatározásoknak meg kell felelniük a Google Play Fejlesztői Programszabályzat előírásainak.
   - Olyan módszert kell kialakítanod, mellyel a hirdetési kreatívok életkornak megfelelő csoportokba sorolhatók. Az életkornak megfelelő csoportokat úgy kell meghatározni, hogy legalább egy „Korhatár nélküli" és egy „Felnőtteknek" csoportot tartalmazzanak. A besorolás módszerét össze kell hangolni a Google SDK-knak biztosított módszertanával, amelyet az SDK-k az érdeklődés jelzésére szolgáló űrlap kitöltése után kapnak meg.
   - Biztosítanod kell, hogy amikor a gyermekek számára történő hirdetésmegjelenítés valós idejű ajánlattétel útján zajlik, megtörténjen a kreatívok ellenőrzése, és hogy ezek megfeleljenek a fenti követelményeknek.
   - Továbbá rendelkezned kell olyan mechanizmussal, amellyel vizuálisan is azonosíthatod a készletedből származó kreatívokat (például vízjellel látod el a hirdetési kreatívot – amely lehet a vállalkozásod látható logója –, vagy ehhez hasonló funkciót alkalmazol).
2. **Hirdetésformátum:** Biztosítanod kell, hogy a gyermekkorú felhasználóknak megjelenített minden hirdetés megfeleljen a Családbarát hirdetésformátumra vonatkozó követelményeknek, és lehetővé kell tenned, hogy a fejlesztők olyan hirdetésformátumokat válasszanak, amelyek megfelelnek a Google Play Családokkal kapcsolatos irányelvének.
   - A hirdetések nem tartalmazhatnak félrevezető tartalmat, és nem szabad őket úgy megtervezni, hogy gyermekkorú felhasználók véletlenül rájuk kattintsanak. Nem engedélyezett az olyan megtévesztő hirdetések használata, amelyek átkattintásra kényszerítik a felhasználókat egy másik hirdetést aktiváló Elvetés gombbal, vagy úgy, hogy hirtelen hirdetést jelenítenek meg az alkalmazás olyan részén, ahová a felhasználó általában valamelyik másik funkció miatt koppint.
   - Nem engedélyezettek a zavaró hirdetések, ideértve azokat a hirdetéseket, amelyek az egész képernyőt elfoglalják, vagy zavarják az alkalmazás szokásos használatát, és nem egyértelmű, hogy miként kell bezárni őket (pl.: Hirdetésfal).
   - Az alkalmazás szokásos használatát vagy a játékmenetet megzavaró hirdetéseknek (beleértve a jutalommal járó vagy opcionális hirdetéseket) öt másodperc után bezárhatónak kell lenniük.
   - Nem helyezhető el több hirdetés egy oldalon. Nem engedélyezett például több szalaghirdetés vagy videóhirdetés megjelenítése, sem olyan szalaghirdetésé, amely több ajánlatot jelenít meg egyetlen elhelyezésen.
   - A hirdetéseknek jól elkülöníthetőnek kell lenniük az alkalmazás tartalmától. Nem engedélyezett az olyan offerwall és képernyőn maradó hirdetési élmény, amelyek a gyermekkorú felhasználók számára nem azonosítható egyértelműen hirdetésként.
   - A hirdetések nem használhatnak megrázó vagy érzelmi manipulációt alkalmazó trükköket, amelyek a megtekintésüket ösztönzik.
3. **Érdeklődésen alapuló hirdetés/remarketing:** Biztosítanod kell, hogy a gyermekkorú felhasználóknak megjelenő hirdetések nem használnak érdeklődésen alapuló hirdetést (olyan egyéni felhasználókra célzott hirdetést, akik online böngészési viselkedési szokásaik alapján bizonyos jellemzőkkel rendelkeznek) vagy remarketinget (egyéni felhasználókra célzott hirdetést az alkalmazással vagy webhellyel kapcsolatos korábbi interakciók alapján).
4. **Adatkezelési gyakorlat:** SDK-szolgáltatóként átláthatóan kell kezelned a felhasználói adatokat (például egy felhasználótól vagy felhasználóról gyűjtött adatok, beleértve az eszközadatokat). Ez alatt azt értjük, hogy közölni kell, hogy az SDK eléri, gyűjti, használja és megosztja az adatokat; valamint az adatok felhasználását a közölt célokra kell korlátozni. Ezek a Google Play-követelmények kiegészítik a vonatkozó adatvédelmi jogszabályok által előírt valamennyi követelményt. Tájékoztatást kell nyújtanod arról, ha alkalmazásod személyes és bizalmas

információkat gyűjt gyermekektől, beleértve, de nem kizárólagosan a hitelesítési adatokat, a mikrofonból és a kamerából származó adatokat, az eszközadatokat, az Android-azonosítót és a hirdetéshasználati adatokat.

- Kérelmenkénti vagy alkalmazásonkénti alapon lehetővé kell tenned a fejlesztőknek a gyermekközpontú bánásmód igénylését a hirdetésmegjelenítéshez. A bánásmódnak meg kell felelnie a vonatkozó jogszabályoknak és rendeleteknek, például az USA gyermekek online adatvédelmére vonatkozó törvényének (Children's Online Privacy and Protection Act; COPPA) és az EU általános adatvédelmi rendeletének (GDPR) .
  - A gyermekközpontú bánásmód részeként a Google Play emellett megköveteli a hirdetési SDK-któl a személyre szabott hirdetések, az érdeklődésen alapuló hirdetések és a remarketing letiltását is.
- Biztosítanod kell, hogy amikor a gyermekek számára való hirdetésmegjelenítés valós idejű ajánlattétel útján zajlik, megtörténjen az adatvédelmi jelzők továbbítása az ajánlattevők számára.
- Nem továbbíthatsz a gyermektől vagy az ismeretlen korú felhasználótól Android-hirdetésazonosítót (AAID), SIM-sorozatszámot, buildsorozatszámot, BSSID-t, MAC-címet, SSID-t, IMEI-t és/vagy IMSI-t.

5. **Közvetítési platformok:** Amikor gyermekeknek jelenítesz meg hirdetéseket, a következőkre kell figyelned:
   - csak családbarát öntanúsító hirdetési SDK-k használhatók, vagy olyan intézkedéseket kell megvalósítani, amelyekkel biztosítható, hogy a közvetítésből származó hirdetések mindegyike megfeleljen ezeknek a követelményeknek; valamint
   - meg kell adni a közvetítési platformok számára szükséges adatokat a hirdetéstartalom besorolásának és a gyermekközpontú bánásmódnak a jelzésére.
6. **Öntanúsítás és megfelelőség:** Elegendő információt kell biztosítanod a Google részére (pl. az érdeklődés jelzésére szolgáló űrlapon jelzett információkat) annak igazolásához, hogy a hirdetési SDK-k irányelvei megfelelnek az összes öntanúsítási követelménynek, beleértve, de nem kizárólagosan a következőket:
   - Biztosítanod kell az SDK-d vagy közvetítési platformod általános szerződési feltételeinek, adatvédelmi irányelveinek és megjelenítők részére szóló integrálási útmutatójának angol nyelvű változatát.
   - Be kell küldened egy mintaként szolgáló tesztalkalmazást, amely a hirdetési SDK legújabb, megfelelő verzióját használja. A mintaként szolgáló tesztalkalmazás teljesen felépített és futtatható androidos APK legyen, amely az SDK összes funkcióját használja. A tesztalkalmazásra vonatkozó követelmények:
     - Teljesen felépített és futtatható, telefonra méretezett androidos APK-ként kell beküldeni.
     - A hirdetési SDK legújabb vagy hamarosan megjelenő verzióját kell használnia, amelynek meg kell felelnie a Google Play irányelveinek.
     - A hirdetési SDK-d összes funkcióját használnia kell, beleértve a hirdetési SDK meghívását hirdetések lekérése és megjelenítése céljából.
     - A tesztalkalmazáson keresztül lekért kreatívok útján teljes körű hozzáféréssel kell rendelkeznie a hálózaton lévő minden élő, illetve megjelenítést végző hirdetéskészlethez.
     - Földrajzi hely alapján nem korlátozható.
     - Ha készleted vegyes közönségnek szól, akkor a tesztalkalmazásodnak képesnek kell lennie megkülönböztetni a teljes készletből, illetve a gyermekek vagy minden korcsoport számára megfelelő készletből származó kreatívokra vonatkozó kérelmeket.
     - Nem korlátozható konkrét hirdetésekre a készleten belül, kivéve, ha a semleges életkorszűrés szabályozza.
7. Időben kell válaszolnod a jövőbeni információkérésekre, és tanúsítanod kell , hogy az összes újonnan kiadott verzió megfelel a legújabb Google Play Fejlesztői Programszabályzatnak, beleértve a Családokkal kapcsolatos irányelvekre vonatkozó követelményeket.

8. **Jogi megfelelőség:** A családbarát, öntanúsított hirdetési SDK-knak olyan hirdetésmegjelenítést kell támogatniuk, amely megfelel a megjelenítőkre érvényes, gyermekekkel kapcsolatos törvényeknek és jogszabályoknak.
   - Gondoskodnod kell arról, hogy az SDK-d vagy közvetítési platformod megfeleljen az USA gyermekek online adatvédelmére vonatkozó törvényének (Children's Online Privacy and Protection Act; COPPA) , az EU általános adatvédelmi rendeletének (GDPR) , valamint minden egyéb vonatkozó jogszabálynak vagy rendeletnek.

     Megjegyzés: A „gyermek” szó mást és mást jelenthet a különböző nyelveken és kontextusokban. Mindenképpen ajánlott jogi tanácsot kérni arra vonatkozóan, hogy milyen kötelezettségek és korhatáros követelmények vonatkozhatnak az alkalmazásra. A fejlesztő tudja a legjobban, hogyan működik az alkalmazása, ezért az ő segítségére hagyatkozunk, hogy biztosak lehessünk abban, hogy a Google Playen megtalálható alkalmazások biztonságosak a családok számára.

További információt a program követelményeivel kapcsolatban a Családbarát öntanúsító hirdetési SDK program oldalon találsz.

Betartatás

Mindig jobb elkerülni az irányelvsértést, de amikor mégis bekövetkezik, minden erőnkkel igyekszünk tájékoztatni a fejlesztőket arról, hogyan tehetik alkalmazásaikat megfelelővé. A felhasználókat arra kérjük, tudassák velünk, ha valamilyen irányelvsértést észlelnek , vagy ha az irányelvsértés kezelésével kapcsolatban kérdéseik vannak.

Az irányelvek hatálya

Irányelveink minden olyan tartalomra vonatkoznak, amelyet az alkalmazás megjelenít, vagy amelyhez linket tartalmaz (ideértve a felhasználók számára megjelenített hirdetéseket is, és minden olyan, felhasználó által létrehozott tartalmat, amelyet az alkalmazás tárol, vagy amelyhez linket tartalmaz). Emellett vonatkozik a fejlesztői fiókjában szereplő összes, a Google Playen nyilvánosan megjelenő tartalomra, beleértve az Ön fejlesztői nevét és a feltüntetett fejlesztői webhely céloldalát.

Nem engedélyezzük az olyan alkalmazásokat, amelyek lehetővé teszik a felhasználóknak, hogy más alkalmazásokat telepítsenek eszközükre. Azoknak az alkalmazásoknak, amelyek más alkalmazásokhoz, játékokhoz vagy szoftverekhez telepítés nélkül biztosítanak hozzáférést, beleértve a harmadik felek által nyújtott szolgáltatásokat és környezeteket is, gondoskodniuk kell arról, hogy az összes olyan tartalom, amelyhez hozzáférést biztosítanak, megfeleljen a Google Play valamennyi irányelvének, továbbá előfordulhat, hogy további irányelv-felülvizsgálatokon is át kell esniük.

A jelen irányelvekben definiált fogalmak jelentése megegyezik a Fejlesztői terjesztési megállapodásban (Developer Distribution Agreement; DDA) definiált fogalmak jelentésével. A jelen irányelvek és a Fejlesztői terjesztési megállapodás betartása mellett az alkalmazás tartalmát tartalombesorolási irányelveinknek megfelelően értékelni kell.

Nem engedélyezünk olyan alkalmazásokat és alkalmazástartalmakat, amelyek aláássák a felhasználóknak a Google Play ökoszisztémájába vetett bizalmát. Számos tényezőt figyelembe veszünk, amikor arról döntünk, hogy az alkalmazások felkerülhetnek-e a Google Playre (vagy eltávolításra kerülnek-e onnan). Ilyen tényező többek között az ismételt kártékony viselkedés és a visszaélés magas kockázata. A visszaélések kockázatát többek között alkalmazás- és fejlesztőspecifikus panaszokkal, hírekkel, korábbi irányelvsértések előzményeivel, felhasználói visszajelzésekkel és népszerű márkák, karakterek és egyéb eszközök használatával azonosítjuk.

A Google Play Protect működése

A Google Play Protect telepítéskor ellenőrzi az alkalmazásokat. Szabályos időközönként az eszközt is megvizsgálja. Ha potenciálisan kártékony alkalmazást talál, akkor a következőket teheti:

- Értesítést küld. Az alkalmazás eltávolításához koppintson az értesítésre, majd az Eltávolítás lehetőségre.
- Letiltja az alkalmazást, amíg a felhasználó el nem távolítja.
- Automatikusan eltávolítja az alkalmazást. Ha a Play Protect kártékony alkalmazást észlel, általában értesítést küld Önnek arról, hogy eltávolította az alkalmazást.

Hogyan működik a rosszindulatú programok elleni védelem?

A harmadik félhez tartozó rosszindulatú szoftverekkel, URL-ekkel és egyéb biztonsági résekkel szembeni védelem érdekében a Google információkat kaphat az alábbiakról:

- az eszköz hálózati kapcsolatai;
- potenciálisan kártékony URL-ek;
- az operációs rendszer és az eszközre a Google Playen vagy más forrásokon keresztül telepített alkalmazások.

Figyelmeztetést kaphat a Google-tól a nem biztonságosnak tűnő alkalmazásokra vagy URL-ekre vonatkozóan. A Google eltávolíthatja az alkalmazást vagy URL-t, illetve meggátolhatja a telepítését, amennyiben tudottan kártékony az eszközökre, adatokra vagy felhasználókra nézve.

Eszköze beállításaiban kikapcsolhat néhányat a fenti védelmi lépések közül. A Google azonban továbbra is kaphat információkat a Google Playen keresztül telepített alkalmazásokról, eszköze pedig továbbra is ellenőrizheti biztonsági okokból a más forrásokból telepített alkalmazásokat anélkül, hogy információt küldene a Google számára.

Az adatvédelmi értesítések működése

Ha a Google Play Áruházból eltávolítunk egy adott alkalmazást, mert hozzáférhet a felhasználók személyes adataihoz, akkor erről a Google Play Protect értesítést küld a felhasználóknak, akik ekkor dönthetnek úgy, hogy eltávolítják eszközükről az alkalmazást.

Megerősítési eljárás

Amikor a tartalmakat vagy fiókokat felülvizsgáljuk annak megállapítása érdekében, hogy sértik-e a jogszabályokat vagy az irányelveinket, a döntés meghozatalakor különböző információkat veszünk figyelembe, beleértve az alkalmazás metaadatait (például az alkalmazás címét, leírását), az alkalmazáson belüli élményt, a fiókinformációkat (például azt, hogy történt-e korábban irányelvsértés), a harmadik felek alkalmazásban használt kódjait, valamint (adott esetben) a bejelentési mechanizmusok, továbbá a saját kezdeményezésű felülvizsgálatok révén rendelkezésre bocsátott egyéb információkat. Felhívjuk a figyelmedet, hogy te vagy felelős annak biztosításáért, hogy a harmadik felek alkalmazásodban használt kódjai (például egy SDK) és ezen harmadik felek alkalmazásodat érintő gyakorlatai megfeleljenek a Google Play Fejlesztői Programszabályzatának.

Ha az alkalmazásod vagy fejlesztői fiókod megsérti valamelyik irányelvünket, az alábbiakban ismertetett módon tesszük meg a megfelelő intézkedést. Emellett releváns információkat küldünk e-mailben arról, hogy milyen intézkedéseket tettünk, és tájékoztatunk arról is, hogy hogyan fellebbezhetsz, ha úgy véled, tévesen intézkedtünk.

Felhívjuk figyelmedet, hogy az eltávolításról szóló és adminisztratív értesítések nem feltétlenül jelzik a fiókban, az alkalmazásban vagy a tágabb alkalmazásportfólióban tetten érhető irányelvsértések mindegyikét. A fejlesztők felelősek az irányelvekkel kapcsolatos problémák kijavításáért, és fokozott gondosságot várunk el tőlük annak biztosítása érdekében, hogy az alkalmazás vagy fiók többi része teljes mértékben megfeleljen az irányelveknek. További betartatási intézkedéseket eszközölhetünk, ha nem hárítod el fiókodban és minden alkalmazásodban az irányelvsértő problémákat.

A jelen irányelvek vagy a Fejlesztői terjesztési megállapodás ismétlődő vagy súlyos megsértése (például csalás, rosszindulatú programok vagy olyan alkalmazások használata, amelyek kárt

okozhatnak a felhasználónak vagy az eszközben) az egyéni vagy kapcsolódó Google Play fejlesztői fiókok megszüntetésével jár.

Betartatási intézkedések

A betartatási intézkedések különféle módokon érinthetik az alkalmazásokat. Emberi és automatizált értékelés kombinációját használjuk az alkalmazások és az alkalmazások tartalmának felülvizsgálatához, hogy észleljük és értékeljük az irányelveinket sértő és a felhasználókra és a Google Play ökoszisztémára nézve káros tartalmakat. Az automatizált modellek használatával több irányelvsértést észlelhetünk, és gyorsabban értékeljük a potenciális problémákat, ami segít abban, hogy a Google Play mindenki számára biztonságos lehessen. Az irányelvsértő tartalmakat vagy eltávolítjuk automatizált modelljeink segítségével, vagy pedig – amennyiben árnyaltabb meghatározásra van szükség – megjelöljük, hogy a tartalom értékelését végző, képzett operátorok és elemzők további vizsgálatot végezzenek, például mert szükség van a tartalom kontextusának megértésére. Ezeknek a manuális felülvizsgálatoknak az eredményével azután kibővítjük a betanítási adatokat gépi tanulási modelljeink továbbfejlesztése érdekében.

A következő szakasz bemutatja, hogy milyen intézkedéseket hajthat végre a Google Play, illetve milyen hatással lesznek az intézkedések az alkalmazásodra és/vagy Google Play fejlesztői fiókodra.

Hacsak a betartatással kapcsolatos adott közlésünkben másként nem szerepel, ezek az intézkedések minden régióra vonatkoznak. Ha például az alkalmazás felfüggesztésére kerül sor, akkor az alkalmazás valamennyi régióban hozzáférhetetlenné válik. Ezen túlmenően – amennyiben az másként nem szerepel – hacsak nem fellebbezel, és a fellebbezésednek helyt nem adunk, ezek az intézkedések hatályban maradnak.

Elutasítás

- Az ellenőrzésre beküldött új alkalmazás vagy alkalmazásfrissítés nem lesz hozzáférhető a Google Playen.
- Meglévő alkalmazás frissítésének elutasítása esetén az alkalmazás frissítés előtt közzétett verziója továbbra is hozzáférhető marad a Google Playen.
- Az elutasítástól függetlenül továbbra is hozzáférhet az elutasított alkalmazás meglévő felhasználói telepítési adataihoz, statisztikáihoz és értékeléseihez.
- Az elutasítás nincs hatással Google Play fejlesztői fiókja állapotára.

Megjegyzés: Csak akkor küldje be újra az elutasított alkalmazást, ha már minden irányelvsértő problémát kijavított.

Eltávolítás

- Az alkalmazás – a korábbi verzióival együtt – el lett távolítva a Google Playről, és a továbbiakban már nem lesz letölthető a felhasználók számára.
- Mivel az alkalmazást eltávolítottuk, a felhasználók nem tudják majd megtekinteni az alkalmazás áruházi adatlapját. Ezeket az információkat visszaállítjuk, ha az eltávolított alkalmazás helyett az irányelveknek megfelelő frissítést küldesz be.
- A felhasználók nem végezhetnek alkalmazáson belüli vásárlásokat, és nem használhatják az alkalmazáson belüli számlázási funkciókat, amíg a Google Play jóvá nem hagyja az irányelveknek megfelelő verziót.
- Az eltávolítás nincs azonnali hatással a Google Play fejlesztői fiók minősítésére, azonban a többszörös eltávolítás felfüggesztést eredményezhet.

Megjegyzés: Csak akkor küldd be újra az eltávolított alkalmazást, ha már minden irányelvsértő problémát kijavítottál.

Felfüggesztés

- Az alkalmazás – a korábbi verzióival együtt – el lett távolítva a Google Playről, és a továbbiakban már nem lesz letölthető a felhasználók számára.
- Felfüggesztésre súlyos vagy többszörös irányelvsértés, illetve alkalmazás többszöri elutasítása vagy eltávolítása következményeként kerülhet sor.
- Mivel az alkalmazást felfüggesztettük, a felhasználók nem tudják majd megtekinteni az alkalmazás áruházi adatlapját.
- A felfüggesztett alkalmazás APK-ját vagy alkalmazáscsomagját a továbbiakban nem használhatod.
- A felhasználóid nem végezhetnek alkalmazáson belüli vásárlást, és nem használhatják az alkalmazáson belüli számlázási funkciókat.
- A felfüggesztések figyelmeztetésnek minősülnek a Google Play fejlesztői fiók jó minősítésének szempontjából. Több figyelmeztetés az egyéni és a kapcsolódó Google Play fejlesztői fiókok megszüntetésével járhat.

Korlátozott láthatóság

- Korlátoztuk az alkalmazás felfedezhetőségét a Google Playen. Az alkalmazás továbbra is rendelkezésre áll a Google Playen, és hozzáférhető az alkalmazás áruházi adatlapjának közvetlen linkjével rendelkező felhasználók számára.
- A korlátozott láthatóság nincs hatással a Google Play fejlesztői fiók állapotára.
- A korlátozott láthatóság nincs hatással arra, hogy a felhasználók meg tudják-e tekinteni az alkalmazás meglévő áruházi adatlapját.

Korlátozott régiók

- Az alkalmazást csak bizonyos régiókban tölthetik le a Google Playről a felhasználók.
- A más régiókban tartózkodó felhasználók nem fogják megtalálni az alkalmazást a Play Áruházban.
- Azok a felhasználók, akik korábban telepítették az alkalmazást, továbbra is használhatják az eszközükön, de már nem fogják megkapni a frissítéseket.
- A régiókorlátozás nincs hatással a Google Play fejlesztői fiók minősítésére.

A fiók korlátozott állapota

- A fejlesztői fiók korlátozott állapotában a fiók katalógusában lévő összes alkalmazás eltávolítása megtörténik a Google Playről, és a fejlesztő a továbbiakban nem tud új alkalmazást közzétenni vagy nem tudja a meglévő alkalmazásokat újból közzétenni. A fejlesztő a Play Console-hoz továbbra is hozzáférhet.
- Mivel a Google valamennyi alkalmazást eltávolította, a felhasználók nem tudják majd megtekinteni az alkalmazás áruházi adatlapját és a fejlesztői profilt.
- Aktuális felhasználóid nem végezhetnek alkalmazáson belüli vásárlást, és nem használhatják az alkalmazáson belüli számlázási funkciókat.
- A Play Console-t továbbra is használhatod arra, hogy további információt közölj a Google Playjel, továbbá hogy módosítsd fiókadataidat.
- Miután valamennyi irányelvsértést kiküszöbölted, az alkalmazásaidat is újra közzé tudod majd tenni.

Fiók megszüntetése

- A fejlesztői fiók megszüntetése esetén a fiókhoz tartozó összes alkalmazást eltávolítjuk a Google Playről, és a fejlesztő a továbbiakban nem tud új alkalmazást közzétenni. Ezzel együtt az összes kapcsolódó Google Play fejlesztői fiókot is véglegesen felfüggesztjük.
- A többszörös felfüggesztések és az irányelvek súlyos megsértése miatti felfüggesztések a Play Console-fiók megszüntetését is eredményezhetik.
- Mivel a megszüntetett fiókhoz tartozó alkalmazásokat eltávolítottuk, a felhasználók nem tudják majd megtekinteni az érintett áruházi adatlapokat és fejlesztői fiókot.

- Aktuális felhasználóid nem végezhetnek alkalmazáson belüli vásárlást, és nem használhatják az alkalmazáson belüli számlázási funkciókat.

Megjegyzés: A fiókok megszüntetése nem kerülhető meg új fiók regisztrálásával. Az új fiókokat is megszüntetjük (a fejlesztői regisztrációs díj visszatérítése nélkül), ezért kérjük, ne próbálkozz új Play Console-fiók regisztrációjával, ha meglévő fiókod megszüntetett állapotban van.

Alvó fiókok

Az alvó fiókok inaktív vagy gazdátlan fejlesztői fiókok. Az alvó fiókok nem jó minősítésűek a Fejlesztői terjesztési megállapodás előírásai szempontjából.

A Google Play fejlesztői fiókok alkalmazásokat közzétevő és azokat rendszeresen karbantartó, aktív fejlesztők számára készültek. A visszaélések elkerülése érdekében megszüntetjük az alvó, nem használt vagy számottevő rendszeres tevékenységet (például alkalmazások közzétételét és frissítését, statisztikákhoz való hozzáférést vagy áruházi adatlapok kezelését) nem mutató fiókokat.

Az alvó fiókok megszüntetésekor a rendszer törli a fiókot és az összes hozzá társított adatot. A regisztrációs díj nem téríthető vissza, és elvész. Mielőtt megszüntetjük az alvó fiókodat, értesítünk erről a fiókhoz megadott kapcsolatfelvételi módon.

Az alvó fiók megszüntetése után is lesz lehetőséged új fiókot létrehozni, ha úgy döntesz, hogy a Google Playen szeretnél közzétenni tartalmakat. Nem aktiválhatod újra a fiókodat, és a korábbi alkalmazások vagy adatok nem fognak rendelkezésre állni az új fióknál.

Az irányelvsértések kezelése és jelentése

Betartatási intézkedés elleni fellebbezés

Ha tévedés történt, és arra a következtetésre jutunk, hogy az alkalmazás nem sérti a Google Play programszabályzatát és a Fejlesztői terjesztési megállapodást, visszaállítjuk az alkalmazást. Ha alaposan átolvastad az irányelveket, és úgy véled, hogy döntésünk téves lehet, akkor a betartatással kapcsolatos e-mailben található utasításokat követve vagy ide kattintva fellebbezhetsz a döntésünk ellen.

További források

Ha további információra van szüksége a betartatási intézkedésekről vagy valamelyik felhasználó értékeléséről/megjegyzéséről, akkor keresse fel az alábbi forrásokat, vagy vegye fel velünk a kapcsolatot a Google Play Súgón keresztül. Jogi tanácsot azonban nem tudunk adni. Ha ilyen tanácsra van szüksége, forduljon jogi tanácsadóhoz.

- Alkalmazás-ellenőrzés
- Az irányelvek megsértésének jelentése
- Kapcsolatfelvétel a Google Playjel fiók megszüntetése vagy alkalmazás eltávolítása miatt
- Tisztességes használatra felszólító figyelmeztetések
- Kifogásolható alkalmazások és megjegyzések jelentése
- Az alkalmazásomat eltávolították a Google Playről
- A Google Play fejlesztői fiókok megszüntetésének magyarázata

---

Play Console-követelmények

Pezsgő alkalmazás-ökoszisztémánk biztonsága érdekében a Google Play minden fejlesztőtől – a fejlesztők Play Console-fiókjához kapcsolódó profilokat is ideértve – megköveteli a Play Console követelményeinek teljesítését. Az ellenőrzött információk a Google Playen jelennek meg, így segítik a

felhasználók fejlesztők iránti bizalmának megteremtését. További információ a Google Playen megjelenített adatokról.

A Google Play kétféle fejlesztői fióktípust kínál: személyes és szervezeti. A megfelelő típusú fejlesztői fiók kiválasztása és a szükséges ellenőrzések elvégzése kulcsfontosságú a zökkenőmentes bevezetési élmény szempontjából. További információ a fejlesztői fiók típusának kiválasztásáról.

A Play Console-fiók létrehozásakor a következő szolgáltatásokat nyújtó fejlesztőknek szervezetként kell regisztrálniuk:

- Pénzügyi termékek és szolgáltatások, többek között például banki szolgáltatás, kölcsön, részvénykereskedés, befektetési alap, szoftveres kriptovaluta-tárca és kriptotőzsde. További információ a pénzügyi szolgáltatásokra vonatkozó irányelvekről.
- Egészségügyi alkalmazások, így például az orvosi jellegű funkciókat felvonultató alkalmazások és az emberi alanyokon végzett kutatásokkal kapcsolatos alkalmazások. További információ az egészségügyi alkalmazások kategóriáiról.
- A VpnService osztály használatára vonatkozóan jóváhagyással rendelkező alkalmazások. További információ a VPN-szolgáltatásra vonatkozó irányelvről.
- Kormányzati alkalmazások, így például a kormányzati szerv által vagy megbízásából kifejlesztett alkalmazások.

A fiók típusának kiválasztását követően a következőket kell tenned:

- Pontosan add meg a fejlesztői fiókra vonatkozó információkat, beleértve a következőket:
  - teljes név és cím;
  - D-U-N-S szám, ha szervezetként regisztrálsz;
  - kapcsolattartási e-mail-cím és telefonszám;
  - adott esetben a Google Play felületén megjelenő fejlesztői e-mail-cím és telefonszám;
  - fizetési módok (adott esetben);
  - a fejlesztői fiókhoz kapcsolt Google fizetési profil;
- ha szervezetként regisztrálsz, győződj meg arról, hogy a fejlesztői fiókod adatai naprakészek és megegyeznek a Dun & Bradstreet-profilodban szereplő adatokkal;

Az alkalmazás beküldése előtt:

- adj meg pontosan minden alkalmazás- és metaadatot;
- töltsd fel az alkalmazás adatvédelmi irányelveit, és töltsd ki az Adatbiztonság szakaszhoz szükséges adatokat;
- adj meg egy aktív demófiókot, annak bejelentkezési adatait és az alkalmazásod Google Play általi felülvizsgálatához szükséges minden egyéb erőforrást (pl.: bejelentkezési hitelesítési adatokat, QR-kódot stb.).

Mint mindig, ügyelned kell arra, hogy az alkalmazás stabil és vonzó legyen, illetve kellőképpen interaktív felhasználói élményt nyújtson. Gondosan kell ellenőrizni, hogy az alkalmazásban minden – a hirdetési hálózatokat, az elemző szolgáltatásokat és a harmadik féltől származó SDK-kat is beleértve – megfeleljen a Google Play Fejlesztői Programszabályzatának; ha pedig az alkalmazás célközönségébe gyermekek is tartoznak, mindenképpen meg kell felelnie a Családokkal kapcsolatos irányelvnek.

Fontos szem előtt tartani, hogy a fejlesztő felelőssége a Fejlesztői terjesztési megállapodás és a teljes Fejlesztői programszabályzat áttekintése annak biztosítása érdekében, hogy az alkalmazás minden követelménynek megfeleljen.

Developer Distribution Agreement

További segítségre van szüksége?
Próbálja ki a következő lépéseket:

Vegye fel velünk a kapcsolatot
Mondja el a részleteket, és segítünk a megoldásban