Norme del programma per gli sviluppatori

(in vigore dal 31 agosto 2024, se non diversamente specificato)

Costruiamo insieme lo store di app e giochi più affidabile al mondo

La tua innovazione è alla base del nostro successo comune, ma comporta anche delle responsabilità. Le presenti Norme del programma per gli sviluppatori, insieme al Contratto di distribuzione per gli sviluppatori, ci garantiscono di poter continuare a offrire le app più innovative e affidabili a oltre un miliardo di persone nel mondo, tramite Google Play. Ti invitiamo a consultare le nostre norme riportate di seguito.

Contenuti con limitazioni

Il servizio Google Play viene utilizzato ogni giorno da persone di tutto il mondo per accedere ad app e giochi. Prima di inviare un'app, occorre stabilire se è adatta a Google Play e se è conforme alle leggi locali.

Rischi per i bambini

Le app che non vietano agli utenti la creazione, il caricamento o la distribuzione di contenuti che agevolano lo sfruttamento o l'abuso di minori saranno soggette alla rimozione immediata da Google Play. È incluso ogni tipo di materiale pedopornografico. Per segnalare contenuti di un prodotto Google che potrebbero configurare lo sfruttamento di un minore, fai clic su **Segnala una violazione** . Se trovi contenuti di questo tipo altrove su Internet, contatta direttamente l'autorità competente nel tuo paese .

È severamente vietato l'uso di app che mettono in pericolo i minori. È vietato quindi, a titolo esemplificativo ma non esaustivo, l'uso di app che promuovono comportamenti volti all'adescamento di minori, quali:

- Interazioni inappropriate rivolte a un minore (ad esempio palpeggiamenti o carezze).
- Adescamento di minori, ad esempio fare amicizia con un minore online per facilitare, online oppure offline, il contatto sessuale e/o lo scambio di immagini di natura sessuale con il minore in questione.
- Sessualizzazione di minori (ad esempio immagini che raffigurano, incoraggiano o promuovono l'abuso sessuale di minori oppure la raffigurazione di minori per favorirne lo sfruttamento sessuale).
- Sextortion (ad esempio, minacciare o ricattare un minore utilizzando l'accesso reale o presunto alle sue immagini intime).
- Traffico di minori (ad esempio, annunci o proposte di sfruttamento sessuale di minori a fini commerciali).

Se veniamo a conoscenza di contenuti che includono materiale pedopornografico, adotteremo le misure necessarie, tra cui la segnalazione al National Center for Missing & Exploited Children. Se ritieni che un minore sia in pericolo o sia stato vittima di abusi, sfruttamento o traffico, contatta le forze dell'ordine locali e una delle organizzazioni dedicate alla sicurezza dei minori indicate qui .

Sono inoltre vietate le app che si rivolgono ai minori, ma contengono temi per adulti incluse, a titolo esemplificativo ma non esaustivo:

- App con eccessiva violenza, sangue e spargimento di sangue.
- App che rappresentano o incoraggiano attività dannose e pericolose.

Non sono ammesse inoltre le app che promuovono una visione negativa del corpo o dell'immagine di sé, incluse app che rappresentano a scopo di intrattenimento chirurgia plastica, perdita di peso e altri interventi di carattere estetico relativi all'aspetto fisico di una persona.

Contenuti inappropriati

Per garantire che Google Play rimanga una piattaforma sicura e rispettosa, abbiamo creato degli standard che definiscono e proibiscono i contenuti dannosi o inappropriati per i nostri utenti.

Contenuti di natura sessuale e linguaggio volgare

Sono vietate le app che contengono o promuovono contenuti di natura sessuale o linguaggio volgare, inclusa la pornografia, o qualsiasi contenuto o servizio inteso alla gratificazione sessuale. Sono vietati le app o i contenuti delle app che sembrano promuovere o richiedere atti sessuali in cambio di un compenso. Sono vietate le app che includono o promuovono contenuti associati a comportamenti volti all'adescamento sessuale o che distribuiscono contenuti di natura sessuale senza consenso. I contenuti che includono nudità possono essere consentiti se il loro scopo principale è formativo, documentaristico, scientifico o artistico e questa nudità non è fine a se stessa.

Le app di cataloghi, ovvero app che elencano titoli di libri/video nell'ambito di un catalogo di contenuti più ampio, possono distribuire libri (inclusi ebook e audiolibri) o titoli di video con contenuti di natura sessuale, a condizione che siano soddisfatti i seguenti requisiti:

- I titoli di libri/video con contenuti di natura sessuale rappresentano una minima parte del catalogo complessivo dell'app.
- L'app non promuove attivamente titoli di libri/video con contenuti di natura sessuale. Questi titoli potrebbero comunque essere visualizzati nei consigli basati sulla cronologia degli utenti o durante promozioni sui prezzi generali.
- L'app non distribuisce titoli di libri/video che contengono contenuti che comportano rischi per i bambini, pornografia o altri contenuti di natura sessuale definiti illegali dalla legge vigente.
- L'app protegge i minorenni limitando l'accesso a titoli di libri/video con contenuti di natura sessuale.

Se un'app ha contenuti che violano queste norme, ma che sono ritenuti appropriati in una regione specifica, l'app potrebbe essere disponibile per gli utenti della regione in questione, ma non sarà disponibile per gli utenti di altre regioni.

Di seguito sono riportati alcuni esempi di violazioni frequenti:

- Rappresentazioni di nudo con connotazione sessuale o atteggiamenti sessualmente allusivi in cui il soggetto è nudo, sfocato o vestito in modo succinto e/o con un abbigliamento che non sarebbe accettabile in un contesto pubblico appropriato.
- Rappresentazioni, animazioni o illustrazioni di atti sessuali o atteggiamenti sessualmente allusivi o rappresentazione avente connotazione sessuale di parti del corpo.
- Contenuti che raffigurano o rappresentano accessori sessuali, guide al sesso, temi sessuali illegali e fetish.
- Contenuti osceni o volgari inclusi, a titolo esemplificativo, contenuti che possono includere linguaggio volgare, insulti, testo esplicito, parole chiave relative a tematiche per adulti/di natura sessuale nella scheda dello Store o nell'app.
- Contenuti che raffigurano, descrivono o promuovono la zoofilia.
- App che promuovono servizi di intrattenimento sessuale, di escort o di altro tipo che potrebbero essere interpretati come un'offerta o una richiesta di atti sessuali in cambio di un compenso inclusi, a titolo esemplificativo, incontri a pagamento o accordi sessuali in cui è previsto o è implicito che uno dei partecipanti fornisca denaro, regali o sostegno economico a un altro partecipante ("sugar dating").
- App che umiliano o trattano le persone come oggetti, ad esempio app che dichiarano di poter mostrare le persone senza vestiti o di vedere attraverso di essi, anche se sono etichettate come app di intrattenimento o per fare scherzi.
- Contenuti o comportamenti che tentano di minacciare o sfruttare le persone presentandole con connotazioni sessuali, ad esempio foto allusive scattate senza consenso, fotocamere nascoste,

contenuti che rappresentano stupri o contenuti di natura sessuale non consensuali creati mediante deepfake o tecnologie simili.

Incitamento all'odio

Sono vietate le app che promuovono la violenza o incitano all'odio nei confronti di individui o gruppi di persone in base a gruppo etnico o origine, religione, disabilità, età, nazionalità, condizione di reduce di guerra, orientamento sessuale, genere, identità di genere, casta, stato di immigrazione o altre caratteristiche associate a discriminazione o emarginazione sistematica.

Le app con contenuti a scopo didattico, documentaristico, scientifico o artistico relativi al nazismo potrebbero essere bloccate in determinati paesi, in conformità con le leggi e normative locali.

Di seguito sono riportati alcuni esempi di violazioni frequenti:

- Contenuti o affermazioni secondo i quali un gruppo protetto è inumano, inferiore o degno di odio.
- App che contengono insulti che incitano all'odio, stereotipi o teorie sulle caratteristiche negative che un gruppo protetto possiederebbe (ad es. spregevole, corrotto, malvagio e così via) o che affermano esplicitamente o implicitamente che tale gruppo rappresenta una minaccia.
- Contenuti o discorsi che mirano a incoraggiare gli altri a credere che determinate persone debbano essere odiate o discriminate perché fanno parte di un gruppo protetto.
- Contenuti che promuovono simboli che incitano all'odio, ad esempio bandiere, simboli, segni di riconoscimento, oggetti correlati o comportamenti associati a gruppi che incitano all'odio.

Violenza

Non sono ammesse app che raffigurano o promuovono scene di violenza gratuita o altre attività pericolose. Sono generalmente ammesse le app che raffigurano scene di violenza fittizia nel contesto di un gioco, ad esempio cartoni animati, caccia o pesca.

Di seguito sono riportati alcuni esempi di violazioni frequenti:

- Raffigurazioni esplicite o descrizioni di scene di violenza realistica o minacce di violenza nei confronti di persone o animali.
- App che promuovono l'autolesionismo, il suicidio, i disturbi alimentari, i giochi di soffocamento o altri atti che possono comportare lesioni gravi o morte.

Estremismo violento

Non consentiamo alle organizzazioni terroristiche o ad altre organizzazioni o movimenti pericolosi coinvolti in atti di violenza contro civili, che hanno preparato atti di questo tipo o ne hanno rivendicato la responsabilità, di pubblicare app su Google Play per alcuno scopo, incluso il reclutamento.

Non sono ammesse app con contenuti correlati all'estremismo violento o contenuti correlati a pianificazione, preparazione o esaltazione della violenza contro i civili, ad esempio contenuti che promuovono atti terroristici, incitano alla violenza o celebrano attacchi terroristici. Per la pubblicazione di contenuti correlati all'estremismo violento a scopo formativo, documentaristico, scientifico o artistico è necessario fornire il contesto pertinente di tali contenuti.

Eventi sensibili

Sono vietate le app che sfruttano o non trattano con la dovuta delicatezza un evento sensibile dall'importante impatto sociale, culturale o politico, ad esempio emergenze civili, disastri naturali, emergenze di salute pubblica, conflitti, decessi o altri eventi tragici. Le app con contenuti correlati a un evento sensibile sono generalmente consentite se tali contenuti hanno un valore a scopo didattico, documentaristico, scientifico o artistico o intendono informare o sensibilizzare le persone in merito all'evento.

Di seguito sono riportati alcuni esempi di violazioni frequenti:

- Mancanza di sensibilità in relazione alla morte per suicidio, overdose, cause naturali e così via di una persona reale o di un gruppo di persone reali.
- Negazione del verificarsi di un evento tragico grave e ben documentato.
- Apparente derivazione di profitto da un evento sensibile senza vantaggi evidenti per le vittime.

Bullismo e molestie

Sono vietate le app che contengono o favoriscono minacce, molestie o atti di bullismo.

Di seguito sono riportati alcuni esempi di violazioni frequenti:

- Bullismo nei confronti di vittime di conflitti internazionali o religiosi.
- Contenuti che configurano tentativi di sfruttamento di altri, inclusi estorsione, ricatto e così via.
- Pubblicazione di contenuti finalizzati alla pubblica umiliazione di un individuo.
- Molestie rivolte alle vittime di un evento tragico o ai loro amici e familiari.

Prodotti pericolosi

Sono vietate le app che favoriscono la vendita di esplosivi, armi da fuoco, munizioni o determinati accessori per armi.

- Gli accessori soggetti a limitazioni sono, ad esempio, quelli che consentono a un'arma da fuoco di simulare colpi automatici o che trasformano un'arma da fuoco in arma automatica (ad esempio bump stock, grilletti a manovella, dispositivi Drop In Auto Sear, kit di conversione) e caricatori o cinture che possono contenere più di 30 proiettili.

Sono vietate le app che forniscono istruzioni per la produzione di esplosivi, armi da fuoco, munizioni, accessori per armi da fuoco soggetti a limitazioni o altre armi. Questo include le istruzioni per trasformare un'arma da fuoco in arma automatica o con capacità di simulazione di colpi automatici.

Marijuana

Sono vietate le app che favoriscono la vendita di marijuana o derivati della marijuana, indipendentemente dalla loro legalità o meno.

Di seguito sono riportati alcuni esempi di violazioni frequenti:

- Permettere agli utenti di ordinare marijuana attraverso una funzionalità del carrello degli acquisti in-app.
- Aiutare gli utenti a organizzare la consegna o il prelievo di marijuana.
- Favorire la vendita di prodotti contenenti THC (tetraidrocannabinolo), inclusi prodotti come oli CBD contenenti THC.

Tabacco e alcol

Sono vietate le app che agevolano la vendita di tabacco o prodotti contenenti nicotina (come sigarette elettroniche, vaporizzatori a penna e bustine di nicotina) o che incoraggiano l'uso illegale o inappropriato di alcolici, tabacco o nicotina.

Informazioni aggiuntive

- Non sono consentite la raffigurazione o l'istigazione al consumo o alla vendita di alcolici o tabacco da parte di minorenni.
- Non è consentito sottintendere che il consumo di tabacco possa migliorare le condizioni sociali, sessuali, professionali, intellettuali o atletiche.
- Non è consentito raffigurare in una luce positiva l'eccessivo consumo di alcolici, inclusa la pratica del "binge drinking" e del "competition drinking".

- Non è consentito pubblicizzare, promuovere o esporre in posizioni di rilievo prodotti correlati al tabacco (sono inclusi annunci, banner, categorie e link che rimandano a siti di vendita di tabacco).
- Potremo consentire la vendita limitata di prodotti correlati al tabacco in app di consegna di alimentari in alcune regioni, soggetta a misure di verifica dell'età (quali il controllo del documento di identità alla consegna).
- Potremo consentire la vendita di prodotti commercializzati come aiuti per smettere di usare nicotina, soggetta a misure di verifica dell'età.

Servizi finanziari

Sono vietate le app che espongono gli utenti a prodotti e servizi finanziari ingannevoli o dannosi.

Agli scopi delle presenti norme vengono considerati prodotti e servizi finanziari quelli relativi alla gestione o all'investimento di denaro e criptovalute, incluse le consulenze personalizzate.

Se l'app contiene o promuove servizi e prodotti finanziari, devi rispettare le normative statali e locali di ogni regione o paese di destinazione dell'app, ad esempio includendo informative specifiche richieste dalla legge locale.

Le app che contengono funzionalità finanziarie devono compilare il relativo modulo di dichiarazione in Play Console.

Opzioni binarie

Non sono ammesse app che forniscono agli utenti la possibilità di scambiare opzioni binarie.

Prestiti personali

Definiamo "prestito personale" l'atto occasionale di prestare denaro, da parte di una persona fisica, organizzazione o persona giuridica a beneficio di un singolo consumatore, non destinato a finanziare l'istruzione personale o l'acquisto di immobilizzazioni. Per prendere decisioni informate in merito all'assunzione di un prestito personale, i consumatori interessati necessitano di informazioni su qualità, caratteristiche, commissioni, piano di rimborso, rischi e benefici del prodotto finanziario.

- Alcuni esempi: prestiti personali, prestiti con anticipo sullo stipendio, prestiti peer-to-peer e prestiti con titolo di proprietà dell'auto in garanzia.
- Esempi non inclusi: mutui, prestiti per l'acquisto di un'auto, linee di credito rotative (ad esempio, carte di credito e linee di credito personali).

Le app che offrono prestiti personali incluse, a titolo esemplificativo, app che offrono prestiti direttamente, generatori di lead e app che mettono in comunicazione i consumatori con prestatori terzi, devono avere la categoria di app impostata su "Finanza" in Play Console e specificare le seguenti informazioni nei metadati:

- Il periodo minimo e massimo per il rimborso.
- Il tasso annuo effettivo globale (TAEG) massimo, che generalmente include il tasso di interesse più commissioni e altri costi annui o altro tasso analogo, calcolato in base alla normativa locale.
- Un esempio rappresentativo del costo totale del prestito, compresi il capitale e tutte le commissioni applicabili.
- Norme sulla privacy che informino in modo esauriente circa l'accesso, la raccolta, l'utilizzo e la condivisione dei dati utente personali e sensibili, soggette alle limitazioni descritte nelle presenti norme.

Sono vietate le app che promuovono prestiti personali che richiedono il rimborso completo entro al massimo 60 giorni dalla data di emissione (i cosiddetti "prestiti personali a breve termine").

Verranno prese in considerazione eccezioni a queste norme per le app per prestiti personali che operano all'interno di paesi in cui regolamenti specifici consentono esplicitamente tali pratiche di

prestito a breve termine in quadri giuridici consolidati. In questi rari casi, le eccezioni verranno valutate in conformità con le leggi locali e le linee guida normative vigenti del rispettivo paese.

Dobbiamo poter stabilire una connessione tra il tuo account sviluppatore ed eventuali licenze o documentazioni fornite che dimostrino la tua idoneità a fornire prestiti personali. Potremmo richiedere ulteriori informazioni o documenti per verificare che il tuo account sia conforme a tutte le leggi e normative locali.

Le app per prestiti personali, le app il cui scopo principale è agevolare l'accesso ai prestiti personali (ad esempio, app per la generazione di lead o per la facilitazione di prestiti) o le app per prestiti accessorie (calcolatori di prestito, guide ai prestiti e così via) e le app di accesso al salario guadagnato (EWA) non sono autorizzate ad accedere a dati sensibili come foto e contatti. Le seguenti autorizzazioni sono vietate:

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

Le app che utilizzano API o informazioni sensibili sono soggette a ulteriori limitazioni e requisiti. Per maggiori informazioni, leggi le norme relative alle autorizzazioni.

Prestiti personali con TAEG elevato

Negli Stati Uniti sono vietate le app per prestiti personali con un tasso annuo effettivo globale (TAEG) pari o superiore al 36%. Le app per prestiti personali negli Stati Uniti devono indicare il TAEG massimo, calcolato in base alla normativa Truth in Lending Act (TILA) .

Questa norma si applica ad app che offrono prestiti direttamente, generatori di lead e app che mettono in comunicazione i consumatori con prestatori di terze parti.

Requisiti specifici dei paesi

Le app di prestiti personali rivolte ai paesi elencati devono rispettare requisiti aggiuntivi e fornire documentazione supplementare nell'ambito della dichiarazione delle funzionalità finanziarie in Play Console. Su richiesta di Google Play, devi fornire informazioni o documenti aggiuntivi relativi alla tua conformità alle normative vigenti e ai requisiti di licenza applicabili.

1. **India**
   - Se la Reserve Bank of India (RBI) ti ha concesso l'autorizzazione a fornire prestiti personali, devi inviarci una copia della licenza per consentirci di esaminarla.
   - Se non ti occupi direttamente di attività di prestito di denaro e offri soltanto una piattaforma per facilitare i prestiti agli utenti da parte di banche o società finanziarie non bancarie registrate (NBFC), devi indicarlo chiaramente nella dichiarazione.
     - Inoltre, i nomi di tutte le banche e NBFC registrate devono essere indicati in modo ben visibile nella descrizione dell'app.
2. **Indonesia**
   - Se la tua app si occupa di servizi di prestiti basati sull'IT ai sensi della normativa OJK num. 77/POJK.01/2016 e successivi aggiornamenti, devi inviare una copia della tua licenza valida per consentirci di esaminarla.
3. **Filippine**

- Tutte le società di finanziamento e prestiti che offrono questi ultimi tramite piattaforme di prestito online devono richiedere un numero di registrazione SEC e il numero di certificato di autorizzazione (CA) alla Philippines Securities and Exchange Commission (PSEC).
  - È inoltre necessario indicare nella descrizione dell'app la ragione sociale, il nome dell'attività, il numero di registrazione PSEC e il certificato di autorizzazione per la gestione di una società di finanziamento e prestiti.
- Le app che riguardano attività di lending crowdfunding, ad esempio il peer-to-peer (P2P) lending, o come definito dai regolamenti e dalle normative che regolano il crowdfunding (Regolamenti CF), devono elaborare le transazioni tramite intermediari CF registrati presso la PSEC.

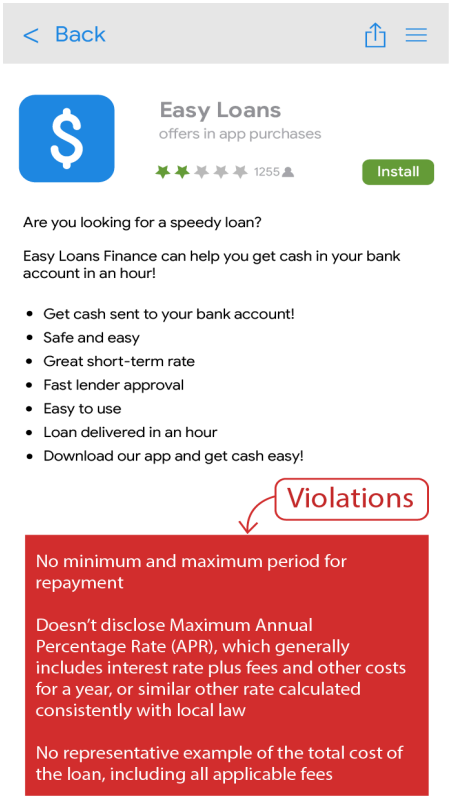
4. **Nigeria**
   - I finanziatori di moneta digitale (DML) devono rispettare e completare il documento LIMITED INTERIM REGULATORY/REGISTRATION FRAMEWORK AND GUIDELINES FOR DIGITAL LENDING del 2022 (che potrebbe essere modificato di tanto in tanto) della Federal Competition and Consumer Protection Commission (FCCPC) nigeriana e ottenere una lettera di approvazione verificabile da questa commissione.
   - Gli aggregatori di prestiti devono fornire la documentazione e/o la certificazione per i servizi di prestiti digitali e i dati di contatto di ogni DML partner.

5. **Kenya**
   - I fornitori di credito digitale (DCP) devono completare la procedura di registrazione DCP e ottenere la licenza dalla Banca centrale del Kenya (CBK). Devi fornire una copia della licenza rilasciata dalla CBK in quanto parte della dichiarazione.
   - Se non ti occupi direttamente di attività di prestito di denaro e offri soltanto una piattaforma per facilitare i prestiti agli utenti da parte di uno o più DCP registrati, devi indicarlo chiaramente nella dichiarazione e fornire una copia della licenza DCP del tuo o dei tuoi partner.
   - Al momento accettiamo solo dichiarazioni e licenze emesse da persone giuridiche e pubblicate nella directory dei fornitori di credito digitale sul sito web ufficiale della CBK.

6. **Pakistan**
   - Ciascuna società finanziaria non bancaria (NBFC) prestatrice può pubblicare solo un'app di prestiti digitali (DLA). Gli sviluppatori che provano a pubblicare più di una DLA per NBFC rischiano la chiusura dell'account sviluppatore e di qualsiasi altro account associato.
   - Per offrire o facilitare servizi di prestiti digitali in Pakistan, devi inviare prove dell'approvazione della SECP.

7. **Thailandia**
   - Le app per prestiti personali rivolte alla Thailandia e con tassi di interesse pari o superiori al 15% devono ottenere una licenza valida dalla Banca di Thailandia (BoT) o dal Ministero delle Finanze (MoF). Gli sviluppatori devono fornire la documentazione a dimostrazione della loro capacità di fornire o agevolare i prestiti personali in Thailandia. Tale documentazione deve includere:
     - Una copia della licenza rilasciata dalla Banca di Thailandia per operare in qualità di fornitore di prestiti personali o di organizzazione di nanofinanza.
     - Una copia della licenza commerciale Pico Finance rilasciata dal Ministero delle Finanze per operare in qualità di finanziatore Pico o Pico-plus.

Di seguito è riportato un esempio di violazione frequente:



Concorsi, giochi e scommesse con vincite in denaro

Sono consentite app di giochi e scommesse con vincite in denaro, annunci correlati a giochi e scommesse con vincite in denaro, programmi fedeltà con elementi basati sulla gamification e app di fantasport giornalieri che soddisfano determinati requisiti.

App di giochi e scommesse

Ai sensi delle limitazioni e nel rispetto di tutte le norme di Google Play, sono ammesse le app che consentono o favoriscono giochi e scommesse online in paesi selezionati, purché lo Sviluppatore completi la procedura di richiesta di iscrizione per le app di giochi e scommesse distribuite su Google Play, sia un operatore statale approvato e/o sia registrato come operatore con licenza presso l'autorità statale competente per giochi e scommesse nel paese in questione e fornisca una licenza di esercizio valida nel paese in questione per il tipo di prodotto di giochi e scommesse online che vuole offrire.

Sono ammesse soltanto app di giochi e scommesse con licenza o autorizzazione valida che includano i seguenti tipi di prodotti di giochi e scommesse online:

- Giochi da casinò online
- Scommesse sportive
- Corse di cavalli (se regolamentate e autorizzate con licenza separatamente dalle scommesse sportive)
- Lotterie
- Fantasport giornalieri

Le app idonee devono soddisfare i seguenti requisiti:

- Lo sviluppatore deve completare correttamente la procedura di richiesta di iscrizione per poter distribuire l'app su Google Play.
- L'app deve essere conforme a tutte le leggi vigenti e agli standard di settore per ogni paese in cui viene distribuita.

- Lo sviluppatore deve disporre di una licenza per giochi e scommesse valida per ogni paese o stato/territorio in cui l'app viene distribuita.
- Lo sviluppatore non deve offrire un tipo di prodotto di giochi e scommesse che non rientra nell'ambito della sua licenza per giochi e scommesse.
- L'app non deve poter essere usata da utenti minorenni.
- L'app non deve poter essere accessibile e utilizzabile in paesi, stati/territori o aree geografiche non coperti dalla licenza per giochi e scommesse fornita dallo sviluppatore.
- L'app NON deve essere acquistabile come app a pagamento su Google Play, né utilizzare la Fatturazione in-app di Google Play.
- L'app deve essere scaricabile e installabile gratuitamente dal Google Play Store.
- L'app deve avere classificazione AO (Adult Only - Solo adulti) o l'equivalente IARC.
- L'app e la relativa scheda devono visualizzare chiaramente le informazioni sulla pratica responsabile di giochi e scommesse.

Altre app per giochi, concorsi e tornei con vincite in denaro

Per tutte le altre app che non rispettano i requisiti di idoneità relativi alle app di giochi e scommesse sopra indicati e che non sono incluse negli "Altri progetti pilota per giochi con vincite in denaro" riportati di seguito, non sono ammessi contenuti o servizi che consentono o favoriscono la capacità degli utenti di puntare, rischiare o partecipare utilizzando denaro reale (inclusi gli articoli in-app acquistati con denaro) per aggiudicarsi un premio di valore monetario reale. Sono inclusi, a titolo esemplificativo, casinò online, scommesse sportive, lotterie, nonché giochi che accettano denaro e offrono premi in denaro o altro valore reale (ad eccezione dei programmi consentiti ai sensi dei requisiti relativi ai programmi fedeltà basati sulla gamification descritti di seguito).

Esempi di violazioni

- Giochi che accettano denaro a fronte dell'opportunità di aggiudicarsi un premio fisico o monetario.
- App con funzionalità o elementi di navigazione (voci di menu, schede, pulsanti, componenti WebView e così via) che offrono un "invito all'azione" per puntare, rischiare o partecipare con denaro a giochi, concorsi o tornei con vincite in denaro, ad esempio app che invitano gli utenti, con frasi come "SCOMMETTI", "REGISTRATI" o "PARTECIPA ANCHE TU", a prendere parte a un torneo per vincere un premio in denaro.
- App che accettano o gestiscono puntate, valute in-app, vincite o versamenti per scommettere per o per aggiudicarsi un premio fisico o monetario.

Altri progetti pilota per giochi con vincite in denaro

A volte potremmo condurre progetti pilota a tempo limitato per alcuni tipi di giochi con vincite in denaro in determinate regioni. Per informazioni dettagliate, visita questa pagina del Centro assistenza. Il progetto pilota relativo alle gru a pesca verticale online in Giappone è terminato l'11 luglio 2023. A partire dal 12 luglio 2023, le app di gru a pesca verticale online potranno essere pubblicate su Google Play a livello globale in base alla legge vigente e a determinati requisiti.

Programmi fedeltà con elementi di gamification

Ove consentito dalla legge e se non sono applicabili requisiti di licenza aggiuntivi per giochi e scommesse, sono consentiti i programmi fedeltà che premiano gli utenti con premi reali o equivalenti in denaro, ai sensi dei seguenti requisiti di idoneità del Play Store:

Per tutte le app (giochi e altri contenuti):

- I vantaggi o i premi del programma fedeltà devono essere chiaramente complementari e subordinati a eventuali transazioni monetarie idonee nell'app (dove la transazione monetaria idonea deve essere una vera e propria transazione separata per fornire beni o servizi indipendenti dal programma fedeltà) e non possono essere subordinati all'acquisto né associati a qualsiasi modalità di scambio

comunque in violazione delle limitazioni previste dalle Norme relative a concorsi, giochi e scommesse con vincite in denaro.

- Ad esempio, nessuna parte della transazione monetaria idonea può rappresentare una tariffa o una scommessa per partecipare al programma fedeltà e la transazione monetaria idonea non deve comportare l'acquisto di beni o servizi a un prezzo superiore al normale.

Per le app di giochi :

- I punti fedeltà o i premi con vantaggi o premi associati a una transazione monetaria idonea possono essere assegnati e riscattati solo in base a un rapporto fisso, che deve essere indicato in modo chiaro nell'app e anche all'interno del regolamento ufficiale del programma disponibile al pubblico. L'acquisizione dei vantaggi o del valore riscattabile **non** può dipendere da scommesse, essere assegnata o moltiplicata in maniera esponenziale in base alle prestazioni nel gioco o a risultati basati su probabilità.

Per le app non di giochi:

- I punti fedeltà o i premi possono essere associati a un concorso o a risultati basati su probabilità se soddisfano i requisiti riportati di seguito. I programmi fedeltà con vantaggi o premi associati a una transazione monetaria idonea devono:
  - Pubblicare il regolamento ufficiale del programma nell'app.
  - Per quanto riguarda i programmi con sistemi di premi casuali, basati su probabilità o variabili, all'interno dei termini ufficiali del programma deve essere indicato quanto segue: 1) le probabilità di qualsiasi programma a premi che usa probabilità fisse per stabilire i premi e 2) il metodo di selezione (ad esempio le variabili usate per stabilire il premio) per tutti gli altri programmi di questo tipo.
  - Specificare un numero fisso di vincitori, una scadenza fissa per l'iscrizione e la data di assegnazione dei premi (per ogni promozione) nei termini ufficiali del programma che preveda estrazioni, concorsi a premi o altre promozioni simili.
  - Indicare in modo chiaro nell'app e nei termini ufficiali del programma qualsiasi rapporto fisso per l'accumulo e il riscatto di premi o punti fedeltà.

Tipo di app con programma fedeltà	**Programma fedeltà con elementi di gamification e premi variabili**	**Premi fedeltà basati su un rapporto o una programmazione fissi**	**Termini e condizioni obbligatori del programma fedeltà**	**I Termini e condizioni devono comunicare le probabilità o il metodo di selezione di qualsiasi programma fedeltà basato su probabilità**
Gioco	Non consentito	Consentiti	Obbligatori	N/A (le app di giochi non possono avere elementi basati su probabilità nei programmi fedeltà)
Contenuti diversi dai giochi	Consentito	Consentiti	Obbligatori	Obbligatorio

Annunci di giochi e scommesse o di giochi, concorsi e tornei con vincite in denaro all'interno di app distribuite su Play

Sono consentite le app con annunci che promuovono giochi e scommesse nonché giochi, concorsi e tornei con vincite in denaro se soddisfano i seguenti requisiti:

- L'app e l'annuncio (inclusi gli inserzionisti) devono essere conformi a tutte le leggi vigenti e agli standard di settore per tutte le località in cui viene visualizzato l'annuncio.

- L'annuncio deve rispettare tutti i requisiti di licenza per gli annunci locali applicabili per tutti i prodotti e servizi relativi a giochi e scommesse oggetto di promozione.
- L'app non deve mostrare annunci relativi a giochi e scommesse a individui di cui sia certa l'età inferiore a 18 anni.
- L'app non deve essere iscritta al programma Per la famiglia.
- L'app non deve essere rivolta a utenti di età inferiore a 18 anni.
- Se pubblicizza un'app di giochi e scommesse (come definita sopra), l'annuncio deve visualizzare chiaramente le informazioni sulla pratica responsabile di giochi e scommesse nella pagina di destinazione, nella scheda dell'app pubblicizzata o all'interno dell'app.
- L'app non deve fornire contenuti di giochi e scommesse simulati (ad es. app di casinò sui social; app con slot machine virtuali).
- L'app non deve fornire funzionalità di supporto o complementari per giochi e scommesse oppure giochi, lotterie e tornei con vincite in denaro (ad esempio funzionalità che agevolano le scommesse, i pagamenti, il tracciamento di risultati/quote sportive/prestazioni o la gestione di fondi di partecipazione).
- I contenuti dell'app non devono promuovere o indirizzare gli utenti a servizi di giochi e scommesse o di giochi, lotterie o tornei con vincite in denaro.

Solo le app che soddisfano tutti i requisiti indicati in questa sezione (in precedenza) possono includere annunci relativi a giochi e scommesse o a giochi, lotterie e tornei con vincite in denaro. Le app di giochi e scommesse accettate (come definite sopra) o le app di fantasport giornalieri accettate (come definite sopra) che soddisfano i requisiti 1-6 sopra elencati possono includere annunci relativi a giochi e scommesse o a giochi, lotterie e tornei con vincite in denaro.

Esempi di violazioni

- Un'app concepita per utenti minorenni e che mostra un annuncio che promuove servizi di giochi e scommesse.
- Un gioco di casinò simulato che promuove o indirizza gli utenti a casinò con denaro reale.
- Un'app dedicata di tracciamento delle quote legate a eventi sportivi contenente annunci di giochi e scommesse integrati che rimandano a un sito di scommesse sportive.
- App che contengono annunci di giochi e scommesse che violano le nostre norme sugli annunci ingannevoli, ad esempio gli annunci che vengono mostrati agli utenti sotto forma di pulsanti, icone o altri elementi in-app interattivi.

App di fantasport giornalieri (DFS)

Sono consentite le app di fantasport giornalieri (DFS), come definito dalle leggi locali vigenti, se soddisfano i seguenti requisiti:

- L'app è 1) distribuita solo negli Stati Uniti o 2) idonea in base ai requisiti delle app per giochi e scommesse e alla procedura di iscrizione sopra indicati per paesi diversi dagli Stati Uniti.
- Lo sviluppatore deve completare la procedura di iscrizione come DFS ed essere accettato per poter distribuire l'app su Play.
- L'app deve essere conforme a tutte le leggi vigenti e gli standard di settore per i paesi in cui è distribuita.
- L'app deve impedire agli utenti minorenni di effettuare scommesse o transazioni monetarie al suo interno.
- L'app NON deve essere acquistabile come app a pagamento su Google Play, né utilizzare la Fatturazione in-app di Google Play.
- L'app deve essere scaricabile e installabile gratuitamente dallo Store.
- L'app deve avere classificazione AO (Adult Only - Solo adulti) o l'equivalente IARC.
- L'app e la relativa scheda devono visualizzare chiaramente le informazioni sulla pratica responsabile di giochi e scommesse.

- L'app deve essere conforme a tutte le leggi vigenti e agli standard di settore per ogni stato o territorio degli Stati Uniti in cui viene distribuita.
- Lo sviluppatore deve disporre di una licenza valida per ciascuno stato o territorio degli Stati Uniti in cui è richiesta una licenza per le app di fantasport giornalieri.
- L'app non deve poter essere utilizzata negli stati o territori degli Stati Uniti in cui lo sviluppatore non possiede la licenza richiesta per le app di fantasport giornalieri; e inoltre
- L'app non deve poter essere utilizzata negli stati o territori degli Stati Uniti in cui le app di fantasport giornalieri non sono legali.

Attività illecite

Sono vietate le app che favoriscono o promuovono attività illegali.

Di seguito sono riportati alcuni esempi di violazioni frequenti:

- Agevolazione della vendita o dell'acquisto di sostanze stupefacenti illegali.
- Raffigurazione o istigazione al consumo o alla vendita di sostanze stupefacenti, alcol e tabacco da parte di minorenni.
- Istruzioni per coltivare o produrre sostanze stupefacenti illegali.

Contenuti generati dagli utenti

I contenuti generati dagli utenti sono contenuti che gli utenti pubblicano in un'app e che sono visibili e accessibili ad almeno un sottoinsieme di utenti dell'app.

Le app che contengono o mostrano contenuti generati dagli utenti, incluse quelle che sono browser o client specializzati che indirizzano gli utenti a una piattaforma di contenuti generati dagli utenti, devono implementare una funzionalità di moderazione dei contenuti generati dagli utenti che sia continua, efficace e robusta e che:

- richieda agli utenti l'accettazione dei Termini e condizioni d'uso e/o dei criteri relativi agli utenti dell'app prima che gli utenti possano creare o caricare contenuti generati dagli utenti;
- definisca contenuti e comportamenti discutibili (in modo conforme alle Norme del programma per gli sviluppatori di Google Play) e li vieti nei Termini e condizioni d'uso o nei criteri relativi agli utenti dell'app;
- moderi i contenuti generati dagli utenti in modo ragionevole e coerente rispetto al tipo di contenuti generati dagli utenti ospitato dall'app. È possibile, ad esempio, fornire un sistema in-app per segnalare e bloccare utenti e contenuti generati dagli utenti discutibili, nonché prendere provvedimenti contro utenti o contenuti generati dagli utenti, ove opportuno. Esperienze diverse con i contenuti generati dagli utenti potrebbero richiedere impegni di moderazione diversi. Ad esempio:
  - Le app che mostrano contenuti generati dagli utenti che identificano un insieme specifico di utenti tramite, ad esempio, la verifica degli utenti o la registrazione offline (come le app usate esclusivamente all'interno di una scuola o un'azienda specifica) devono fornire una funzionalità in-app per la segnalazione di contenuti e utenti.
  - Le funzionalità dei contenuti generati dagli utenti che consentono l'interazione 1:1 tra utenti specifici (ad esempio tramite messaggi diretti, tagging, menzioni e così via) devono fornire una funzionalità in-app per il blocco degli utenti.
  - Le app che danno accesso a contenuti generati dagli utenti pubblicamente accessibili, quali app di social network e app di blog, devono implementare funzionalità in-app per la segnalazione di utenti e contenuti e per il blocco degli utenti.
  - Nel caso di app di realtà aumentata (AR), la moderazione dei contenuti generati dagli utenti (incluso il sistema di segnalazione in-app) deve tenere conto sia di contenuti AR generati dagli utenti che sono discutibili (ad esempio, un'immagine AR sessualmente esplicita) sia della

posizione di ancoraggio AR sensibile (ad esempio, contenuti AR ancorati a un'area con restrizioni, come una base militare o una proprietà privata in cui l'ancoraggio AR potrebbe causare problemi al titolare della proprietà).
- fornisca salvaguardie per impedire che la monetizzazione in-app incoraggi comportamenti discutibili da parte degli utenti.

Contenuti di natura sessuale accidentali

I contenuti di natura sessuale sono considerati "accidentali" se vengono visualizzati in un'app con contenuti generati dagli utenti che (1) dà accesso a contenuti essenzialmente non di natura sessuale e (2) non promuove o consiglia attivamente contenuti di natura sessuale. I contenuti di natura sessuale definiti illegali dalla legge vigente e i contenuti che comportano rischi per i bambini non sono considerati "accidentali" e non sono consentiti.

Le app con contenuti generati dagli utenti possono includere contenuti di natura sessuale accidentali se vengono soddisfatti tutti i seguenti requisiti:

- Questi contenuti sono nascosti per impostazione predefinita tramite filtri che per poter essere disattivati completamente richiedono almeno due azioni dell'utente (ad esempio, i contenuti sono nascosti da un interstitial oppure non possono essere visualizzati per impostazione predefinita a meno che non venga disattivata la funzionalità SafeSearch).
- A bambini e ragazzi, come definito nelle Norme per le famiglie, è espressamente vietato accedere alla tua app tramite l'uso di sistemi di controllo dell'età quali il filtro di controllo dell'età o un sistema appropriato in base a quanto definito dalla legge vigente.
- L'app dà risposte accurate al questionario per la classificazione dei contenuti in merito ai contenuti generati dagli utenti, come richiesto dalle norme relative alla classificazione dei contenuti.

Le app il cui scopo principale è la pubblicazione di contenuti discutibili generati dagli utenti saranno rimosse da Google Play. Analogamente, saranno rimosse da Google Play le app che finiscono per essere utilizzate principalmente per ospitare contenuti discutibili generati dagli utenti oppure che diventano note come luogo in cui vengono creati e diffusi questi contenuti.

Di seguito sono riportati alcuni esempi di violazioni frequenti:

- Promozione di contenuti generati dagli utenti sessualmente espliciti, inclusa l'implementazione o l'autorizzazione di funzionalità a pagamento che incoraggiano principalmente la condivisione di contenuti discutibili.
- App con contenuti generati dagli utenti prive di sufficienti misure di salvaguardia da minacce, molestie o atti di bullismo, in particolare nei confronti di minorenni.
- Post, foto o commenti all'interno di un'app principalmente finalizzati a molestare o prendere di mira un'altra persona sottoponendola a maltrattamenti, attacchi crudeli o atti di derisione.
- App che non procedono ripetutamente alla risoluzione dei reclami degli utenti relativi ai contenuti discutibili.

Servizi e contenuti sanitari

Sono vietate le app che espongono gli utenti a servizi e contenuti sanitari dannosi.

Se l'app contiene o promuove servizi e contenuti sanitari, è necessario assicurarsi che l'app rispetti eventuali leggi e normative vigenti.

App per la salute

Se la tua app accede a dati sanitari ed è un'app per la salute o offre funzionalità correlate alla salute, deve rispettare le norme per gli sviluppatori di Google Play esistenti, tra cui le norme relative a privacy, comportamento ingannevole e abuso del dispositivo e le norme relative agli eventi sensibili, oltre ai seguenti requisiti:

- **Dichiarazione di Play Console:**
  - Vai alla pagina Contenuti app (Norme > Contenuti app) in Play Console e seleziona la categoria o le categorie a cui appartiene la tua app.
- **Norme sulla privacy e requisiti relativi alle informative ben visibili:**
  - Per l'app è necessario pubblicare le norme sulla privacy inserendo un link nel relativo campo in Play Console e tramite un link o un testo all'interno dell'app stessa. Assicurati che le norme sulla privacy siano disponibili su un URL attivo, pubblicamente accessibile e al di fuori di recinti virtuali (non PDF) e che non possano essere modificate (in base alla sezione Sicurezza dei dati).
  - Le norme sulla privacy dell'app, insieme a eventuali informative in-app, devono spiegare in modo esauriente l'accesso, la raccolta, l'utilizzo e la condivisione di dati utenti personali o sensibili, non soltanto quelli indicati nella sezione Sicurezza dei dati in alto. Per le funzionalità o i dati regolamentati da autorizzazioni pericolose o di runtime , l'app deve rispettare tutti i requisiti di consenso e visibilità dell'informativa vigenti.
  - Le autorizzazioni non necessarie per la funzionalità di base di un'app per la salute non devono essere richieste e le autorizzazioni inutilizzate devono essere rimosse. Per consultare l'elenco delle autorizzazioni considerate attinenti all'ambito dei dati sensibili correlati alla salute, vai all'articolo Categorie di app per la salute e informazioni aggiuntive.
  - Se la tua app non è principalmente un'app per la salute, ma ha funzionalità correlate alla salute e accede a dati sanitari, rientra comunque nell'ambito delle norme relative alle app per la salute. Dovrebbe essere chiaro all'utente il collegamento tra la funzionalità di base dell'app e la raccolta di dati correlati alla salute (ad esempio, compagnie assicurative e app di gioco che raccolgono dati sulle attività di un utente per avanzare nel gameplay e così via). Le norme sulla privacy dell'app devono rispecchiare questo uso limitato.
- **Requisiti aggiuntivi:**
  Se la tua app per la salute rientra in una delle classificazioni riportate di seguito, devi rispettare i requisiti pertinenti oltre a selezionare la categoria appropriata in Play Console:
  - **App per la salute affiliate al governo:** se il governo o un'organizzazione sanitaria riconosciuta ti ha autorizzato a sviluppare e distribuire un'app in affiliazione con loro, devi inviare una prova dell'idoneità tramite il modulo di preavviso.
  - **App di tracciamento dei contatti/relative alla condizione di salute:** se la tua app è un'app di tracciamento dei contatti e/o relativa alla condizione di salute, seleziona "Prevenzione di malattie e salute pubblica" in Play Console e fornisci le informazioni richieste tramite il modulo di preavviso precedente.
  - **App di ricerche su soggetti umani:** le app che svolgono ricerche relative alla salute su soggetti umani devono rispettare tutte le regole e i regolamenti, inclusi, a titolo esemplificativo, l'ottenimento del consenso informato dei partecipanti o, in caso di minorenni, di un loro genitore o tutore. Le app di ricerche relative alla salute devono anche avere l'approvazione di un organismo come l'Institutional Review Board (IRB) e/o di un comitato etico indipendente equivalente, salvo eventuali esenzioni. È necessario fornire prove di questa approvazione su richiesta.
  - **App di dispositivi medici o SaMD:** le app considerate dispositivi medici o SaMD devono ottenere e conservare una lettera di autorizzazione o un altro documento di approvazione rilasciati da un ente o un'autorità di regolamentazione responsabile della gestione e della conformità delle app per la salute. È necessario fornire prove di questa autorizzazione o approvazione su richiesta.

Dati di Connessione Salute

I dati a cui accedi tramite le autorizzazioni di Connessione Salute sono considerati dati utente personali e sensibili soggetti alle norme relative ai dati utente nonché ai seguenti requisiti aggiuntivi .

Farmaci con obbligo di prescrizione medica

Sono vietate le app che agevolano la vendita o l'acquisto di farmaci con obbligo di prescrizione medica senza prescrizione.

Sostanze non approvate

Google Play non consente app che promuovono o vendono sostanze non approvate, a prescindere da qualsiasi rivendicazione di legittimità.

Di seguito sono riportati alcuni esempi di violazioni frequenti:

- Tutte le voci di questo elenco non esaustivo di prodotti farmaceutici e integratori vietati .
- Prodotti contenenti efedra.
- Prodotti contenenti gonadotropina corionica umana (hCG) in collegamento con la perdita di peso o il controllo del peso o se pubblicizzati in combinazione con steroidi anabolizzanti.
- Integratori a base di erbe e dietetici che contengono principi attivi farmaceutici o ingredienti pericolosi.
- Indicazioni false o fuorvianti sulla salute, comprese le dichiarazioni che lasciano intendere che un prodotto è efficace quanto farmaci con obbligo di prescrizione medica o sostanze controllate.
- Prodotti non approvati da enti statali, commercializzati in modo da lasciare intendere che siano sicuri o efficaci nel prevenire o curare una malattia o disturbo della salute.
- Prodotti che sono stati oggetto di un'azione o di un avviso da parte di un'autorità legislativa o regolamentare.
- Prodotti i cui nomi possono essere confusi con quelli di sostanze controllate oppure di prodotti farmaceutici o integratori non approvati.

Per ulteriori informazioni sui prodotti farmaceutici e sugli integratori non approvati o fuorvianti che monitoriamo, visita la pagina www.legitscript.com .

Disinformazione sanitaria

Sono vietate le app contenenti informazioni sanitarie fuorvianti che contraddicono la posizione condivisa corrente nel settore medico o che possono danneggiare gli utenti.

Di seguito sono riportati alcuni esempi di violazioni frequenti:

- Affermazioni ingannevoli riguardo ai vaccini, ad esempio che i vaccini possono alterare il DNA di una persona.
- Supporto di trattamenti dannosi e non approvati.
- Supporto di altre pratiche sanitarie dannose, ad esempio le terapie di conversione.

Funzionalità mediche

Non sono consentite app con funzionalità mediche o relative alla salute ingannevoli o potenzialmente dannose. Ad esempio, non sono consentite le app che dichiarano di avere funzionalità di saturimetria basate esclusivamente sull'app. Perché un'app possa misurare la saturazione dell'ossigeno, deve essere supportata da sensori hardware esterni, indossabili o incorporati nello smartphone progettati per questa specifica funzionalità. Nei metadati di queste app supportate devono inoltre essere presenti limitazioni di responsabilità che dichiarino che le app non sono destinate all'utilizzo medico, sono pensate esclusivamente per finalità generiche relative ad attività fisica e benessere e non sono dispositivi medici. Per queste app è inoltre necessario indicare in modo appropriato il modello di dispositivo/hardware compatibile.

Pagamenti - Servizi clinici

Le transazioni che riguardano servizi clinici regolamentati non devono utilizzare il sistema di fatturazione di Google Play. Per ulteriori informazioni, consulta Informazioni sulle norme relative ai pagamenti di Google Play .

Contenuti basati su blockchain

Poiché la tecnologia di blockchain è in rapida e costante evoluzione, il nostro obiettivo è quello di offrire una piattaforma per sviluppatori per stimolare l'innovazione e creare esperienze ottimizzate e più immersive per gli utenti.

Agli scopi delle presenti norme per contenuti basati su blockchain si intendono asset digitali tokenizzati assicurati a una blockchain. Se la tua app include contenuti basati su blockchain, devi rispettare questi requisiti.

Scambi di criptovalute e portafogli software

L'acquisto, il possesso o lo scambio di criptovalute deve avvenire tramite servizi certificati in giurisdizioni regolate.

Inoltre, devi rispettare i regolamenti vigenti in tutti i paesi o le regioni a cui si rivolge la tua app ed evitare di pubblicare l'app dove i tuoi prodotti e servizi sono proibiti. Google Play potrà chiederti di fornire informazioni o documenti aggiuntivi relativi alla tua conformità alle normative vigenti e ai requisiti di licenza applicabili.

Cryptomining

Sono vietate le app che consentono il mining di criptovaluta sui dispositivi. Sono consentite le app che gestiscono da remoto il mining di criptovaluta.

Requisiti di trasparenza per la distribuzione di asset digitali tokenizzati

Se la tua app vende o consente agli utenti di ottenere asset digitali tokenizzati, devi dichiararlo nel modulo di dichiarazione delle funzionalità finanziarie nella pagina Contenuti app di Play Console.

Quando crei un prodotto in-app, nei dettagli del prodotto devi indicare che si tratta di una risorsa digitale tokenizzata. Per indicazioni aggiuntive, consulta l'articolo Creare un prodotto in-app.

Non è consentito promuovere potenziali entrate derivanti da attività di gioco o trading.

Requisiti aggiuntivi per la gamification dell'NFT

Come richiesto dalle norme relative a concorsi, giochi e scommesse con vincite in denaro di Google Play, le app di giochi e scommesse che integrano asset digitali tokenizzati, come gli NFT, devono completare la procedura di richiesta.

Per tutte le altre app che non rispettano i requisiti di idoneità relativi alle app di giochi e scommesse e che non sono incluse negli Altri progetti pilota per giochi con vincite in denaro, non devono essere accettati beni con un valore monetario in cambio della possibilità di ottenere un NFT di valore sconosciuto. Gli NFT acquistati dagli utenti dovrebbero essere consumati o utilizzati nel gioco per migliorare l'esperienza dell'utente o per aiutare gli utenti ad avanzare nel gioco. Gli NFT non devono essere usati per scommettere o giocare per avere l'opportunità di aggiudicarsi un premio di valore monetario reale (inclusi altri NFT).

Di seguito sono riportati alcuni esempi di violazioni frequenti:

- Le app che vendono bundle di NFT senza comunicare i contenuti e i valori specifici degli NFT.
- I giochi da casinò social a pagamento, ad esempio slot machine, che offrono NFT in premio.

Contenuti creati con l'IA

Man mano che i modelli di IA generativa diventano disponibili su più ampia scala per gli sviluppatori, potrai incorporarli nelle tue app per aumentare il coinvolgimento e migliorare l'esperienza utente. Google Play vuole contribuire a garantire che i contenuti creati con l'IA siano sicuri per tutti gli utenti e che i feedback di questi ultimi vengano presi in considerazione per consentire un'innovazione responsabile.

Contenuti creati con l'IA

I contenuti creati con l'IA sono contenuti creati da modelli di IA generativa in base ai prompt degli utenti. Ecco alcuni esempi di contenuti creati con l'IA:

- Chatbot di IA generativa conversazionale da testo a testo, dove l'interazione con il chatbot è una funzionalità centrale dell'app
- Immagine generata dall'IA in base a prompt di testo, immagini o vocali

Per garantire la sicurezza degli utenti e in conformità con la Copertura delle norme di Google Play, le app che generano contenuti usando l'IA devono rispettare le norme per gli sviluppatori di Google Play esistenti, anche vietando e prevenendo la generazione di contenuti con limitazioni, quali i contenuti che agevolano lo sfruttamento o l'abuso di minori, nonché di contenuti che favoriscono un comportamento ingannevole.

Le app che generano contenuti usando l'IA devono contenere funzionalità in-app di segnalazione che consentano agli utenti di segnalare contenuto offensivo agli sviluppatori senza dover uscire dall'app. Gli sviluppatori devono utilizzare le segnalazioni degli utenti per la definizione di filtri e moderazione dei contenuti nelle loro app.

Proprietà intellettuale

Sono vietati gli account sviluppatore e le app che violano i diritti di proprietà intellettuale di altri (inclusi i diritti relativi a marchi, copyright, brevetti, segreti industriali e altri diritti di proprietà). Sono inoltre vietate le app che istigano o inducono alla violazione di diritti di proprietà intellettuale.

Risponderemo a chiare notifiche di presunta violazione del copyright. Per ulteriori informazioni o per presentare una richiesta ai sensi del DMCA (Digital Millennium Copyright Act, Legge statunitense sul copyright), consulta le procedure di Google relative al copyright .

Per presentare un reclamo relativo alla vendita o alla promozione di articoli contraffatti all'interno di un'app, invia una notifica di contraffazione .

I proprietari di marchi che ritengono che su Google Play sia presente un'app che viola i loro diritti sul marchio sono invitati a risolvere la questione contattando direttamente lo sviluppatore. Qualora non riescano a giungere a una soluzione con lo sviluppatore, i proprietari di marchi sono invitati a inviare un reclamo relativo al marchio utilizzando questo modulo .

Se si dispone della documentazione scritta che dimostra l'autorizzazione a utilizzare la proprietà intellettuale di terze parti nella propria app o scheda dello Store (ad esempio marchi, loghi e risorse grafiche), contattare il team di Google Play prima di inviare i contenuti per assicurarsi che l'app non venga rifiutata per violazione di una proprietà intellettuale.

Utilizzo non autorizzato di contenuti protetti da copyright

Le app che violano il copyright sono vietate. Anche la modifica di contenuti protetti da copyright potrebbe essere considerata una violazione. Agli sviluppatori potrebbe essere chiesto di fornire prove a dimostrazione dei loro diritti di utilizzo dei contenuti protetti da copyright.

È opportuno prestare attenzione quando vengono utilizzati contenuti protetti da copyright per dimostrare la funzionalità della propria app. In genere l'approccio più sicuro consiste nel creare contenuti originali.

Di seguito sono riportati alcuni esempi di violazioni frequenti:

- Immagini di copertina di album musicali, videogiochi e libri.
- Immagini di marketing di film, programmi TV o videogiochi.
- Artwork o immagini di fumetti, cartoni animati, film, video musicali o programmi TV.
- Loghi di università e di squadre sportive professionali.

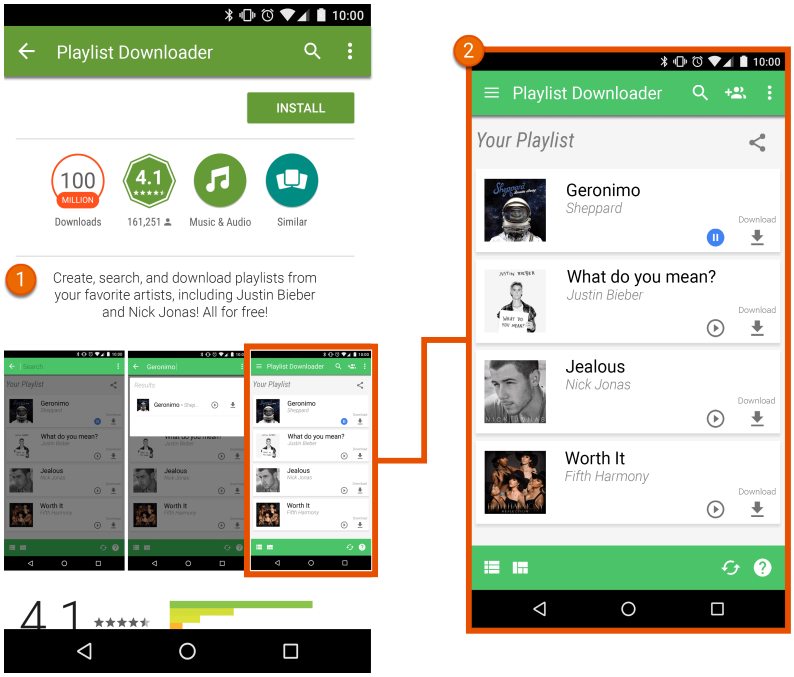
- Foto recuperate dall'account dei social media di un personaggio pubblico.
- Immagini professionali di personaggi pubblici.
- Riproduzioni o "fan art" indistinguibili dall'opera originale protetta da copyright.
- App con tavole armoniche che consentono di ascoltare clip audio di contenuti protetti da copyright.
- Riproduzioni o traduzioni complete di libri che non sono di pubblico dominio.

Istigazione alla violazione del copyright

Le app che inducono o istigano alla violazione del copyright sono vietate. Prima di pubblicare un'app, occorre capire se potrebbe istigare alla violazione del copyright e, se necessario, rivolgersi a un consulente legale.

Di seguito sono riportati alcuni esempi di violazioni frequenti:

- App di streaming che consentono agli utenti di scaricare una copia locale di contenuti protetti da copyright senza autorizzazione.
- App che esortano gli utenti a riprodurre in streaming e scaricare opere protette da copyright, inclusi video e musica, violando così la legge sul copyright vigente:



① La descrizione nella scheda di questa app esorta gli utenti a scaricare contenuti protetti da copyright senza autorizzazione.
② Lo screenshot nella scheda dell'app esorta gli utenti a scaricare contenuti protetti da copyright senza autorizzazione.

Violazione dei marchi

Le app che violano i marchi di altre persone sono vietate. Un marchio è una parola, un simbolo o una combinazione di entrambi che identifica l'origine di un bene o servizio. Una volta acquisito, un marchio conferisce al proprietario diritti esclusivi per il suo utilizzo rispetto a determinati beni o servizi.

La violazione di un marchio consiste nell'utilizzo improprio o non autorizzato di un marchio identico o simile a un altro, in modo tale da creare confusione in merito all'origine del prodotto che rappresenta. Se l'app utilizza marchi di un'altra parte in un modo che rischia di creare confusione, tale app potrebbe essere sospesa.

Contraffazione

Sono vietate le app che vendono o promuovono la vendita di articoli contraffatti. Gli articoli contraffatti contengono un marchio o un logo identico o sostanzialmente non distinguibile da un marchio esistente. Questi articoli imitano gli elementi distintivi del brand del prodotto nel tentativo di essere confusi con il prodotto originale del proprietario del brand.

Privacy, comportamento ingannevole e abuso del dispositivo

Ci impegniamo a fornire un ambiente sicuro per i nostri utenti e a proteggere la loro privacy. Le app ingannevoli, dannose o finalizzate all'utilizzo improprio o illecito di reti, dispositivi o dati personali sono severamente vietate.

Dati utente

Devi assicurare la trasparenza in merito alla modalità di gestione dei dati utente (ad esempio le informazioni fornite da un utente o raccolte in relazione a un utente, incluse le informazioni del dispositivo). Ciò significa divulgare accesso, raccolta, utilizzo, trattamento e condivisione dei dati utente dalla tua app e limitare l'utilizzo dei dati agli scopi conformi alle norme dichiarati. Tieni presente che qualsiasi trattamento di dati utente personali e sensibili è inoltre soggetto ai requisiti aggiuntivi nella sezione "Dati utente personali e sensibili" di seguito. I presenti requisiti di Google Play si aggiungono a quelli previsti dalle leggi vigenti in materia di privacy e protezione dei dati.

Se nell'app includi un codice di terze parti (ad esempio, un SDK), devi garantire che questo codice e le procedure di terze parti che rispettano i dati utente nella tua app siano conformi alle Norme del programma per gli sviluppatori di Google Play, che includono i requisiti relativi alle informative e all'utilizzo. Ad esempio, devi assicurarti che i tuoi provider di SDK non vendano dati utente personali e sensibili recuperati dalla tua app. Questo requisito si applica a prescindere se i dati utenti vengono trasferiti dopo essere stati inviati a un server o tramite l'incorporamento di un codice di terze parti nella tua app.

Dati utente personali e sensibili

I dati utente personali e sensibili includono, a titolo esemplificativo, informazioni che consentono l'identificazione personale, dati finanziari e di pagamento, dati di autenticazione, rubrica, contatti, posizione del dispositivo , dati relativi a SMS e chiamate, dati sulla salute e dati di Connessione Salute , inventario di altre app installate sul dispositivo, dati relativi a microfono e fotocamera, nonché altri dati sensibili del dispositivo o sull'utilizzo. Se la tua app gestisce dati utente personali e sensibili:

- Devi limitare accesso, raccolta, utilizzo e condivisione di dati utente personali e sensibili acquisiti tramite l'app a funzionalità di app e servizi e scopi conformi alle norme ragionevolmente previste dall'utente come segue.
  - Le app che estendono l'utilizzo dei dati utente personali e sensibili per la pubblicazione di annunci devono essere conformi alle norme relative agli annunci di Google Play.
  - Inoltre puoi trasferire i dati secondo necessità ai fornitori di servizi o per motivi legali, come la conformità a una richiesta del governo valida, la legge vigente o in quanto parte di una fusione o acquisizione con avviso legalmente adeguato agli utenti.
- Devi gestire tutti i dati utente personali e sensibili in sicurezza, compresa la loro trasmissione utilizzando metodi moderni di crittografia (ad esempio, tramite HTTPS).
- Devi utilizzare una richiesta di autorizzazioni di runtime ogni qual volta sia disponibile, prima di accedere ai dati controllati tramite autorizzazioni Android .
- Non devi vendere dati utente personali e sensibili.
  - Per "vendita" si intende lo scambio o il trasferimento di dati utente personali e sensibili a una terza parte per un corrispettivo monetario.

- Non viene inteso come vendita il trasferimento avviato dagli utenti di dati utente personali e sensibili, ad esempio, quando un utente usa una funzionalità dell'app per trasferire un file a una terza parte o quando sceglie di usare un'app di studio per scopi dedicati.

Requisito di consenso e informativa ben visibile

Nei casi in cui accesso, raccolta, utilizzo o condivisione di dati utente personali e sensibili da parte della tua app non rientrino nelle ragionevoli previsioni dell'utente in merito al prodotto o alla funzionalità in questione (ad esempio, se la raccolta dei dati avviene in background quando l'utente non interagisce con l'app), devi rispettare i seguenti requisiti:

Informativa ben visibile: devi fornire un'informativa in-app relativa ad accesso, raccolta, utilizzo e condivisione dei dati. L'informativa in-app:

- Deve trovarsi all'interno dell'app, non soltanto su un sito web o nella descrizione dell'app stessa.
- Deve essere visualizzata durante il normale utilizzo dell'app e non deve richiedere all'utente di aprire un menu o le impostazioni.
- Deve descrivere i dati a cui l'app ha accesso o che raccoglie.
- Deve spiegare in che modo i dati verranno utilizzati e/o condivisi.
- Non può essere inserita esclusivamente nelle norme sulla privacy o nei termini di servizio.
- Non può essere inclusa in altre informative non correlate alla raccolta di dati utente personali e sensibili.

Autorizzazioni di runtime e consenso: le richieste per il consenso degli utenti in-app e per le autorizzazioni di runtime devono essere immediatamente precedute da un'informativa in-app che rispetta i requisiti di questa norma. La richiesta di consenso dell'app:

- Deve presentare la finestra di dialogo per il consenso in modo chiaro e inequivocabile.
- Deve richiedere un intervento dell'utente (ad esempio, tocco per accettazione, selezione di una casella di controllo).
- Non deve considerare l'uscita dalla finestra contenente l'informativa (ad esempio, tocco fuori dalla finestra oppure pressione del pulsante Home o Indietro) come espressione del consenso.
- Non deve utilizzare messaggi con scadenza o chiusura automatica per ottenere il consenso dell'utente.
- Deve essere concessa dall'utente prima che la tua app possa iniziare a raccogliere dati utente personali o sensibili o accedervi.

Le app che si basano su altri punti legali per il trattamento di dati utente personali e sensibili senza consenso, come un interesse legittimo ai sensi del GDPR dell'UE, devono rispettare tutti i requisiti legali applicabili e fornire informative appropriate agli utenti, tra cui informative in-app come richiesto da questa norma.

Per rispettare i requisiti delle norme, è consigliabile fare riferimento al formato di esempio che segue per l'Informativa ben visibile, quando richiesta:

- "[Questa app] raccoglie/trasmette/sincronizza/memorizza [tipo di dati] per consentire ["funzionalità"], [in quale scenario]."
- *Esempio: "Fitness Funds raccoglie dati sulla posizione per consentire il monitoraggio dell'attività fisica anche quando l'app è chiusa o non in uso. Questi dati vengono usati anche per la pubblicità".*
- *Esempio: "Call buddy raccoglie dati del registro chiamate in lettura e scrittura per consentire l'organizzazione dei contatti anche quando l'app non è in uso".*

Se la tua app integra un codice di terze parti (ad esempio, un SDK) progettato per raccogliere dati utente personali e sensibili per impostazione predefinita, entro 2 settimane dalla ricezione di una richiesta di Google Play (o, se la richiesta di Google Play prevede un periodo di tempo maggiore, entro questo periodo) devi fornire prove sufficienti a dimostrare che la tua app soddisfa i requisiti di consenso e visibilità dell'informativa di questa norma, ad esempio in relazione ad accesso, raccolta, utilizzo o condivisione dei dati tramite il codice di terze parti.

Di seguito sono riportati alcuni esempi di violazioni frequenti:

- Un'app che raccoglie la posizione del dispositivo, ma non ha un'informativa ben visibile che spiega quale funzionalità usa questo dato e/o indica l'utilizzo in background dell'app.
- Un'app ha un'autorizzazione di runtime che richiede l'accesso ai dati prima dell'informativa ben visibile che specifica per quali finalità vengono usati i dati.
- Un'app che accede all'inventario di un utente delle app installate e non tratta questi dati come personali o sensibili e soggetti alle suddette Norme sulla privacy e ai requisiti sopra indicati di gestione dei dati, Informativa ben visibile e Consenso.
- Un'app che accede ai dati del telefono o della rubrica di contatti di un utente e non tratta questi dati come personali o sensibili e soggetti alle suddette Norme sulla privacy e ai requisiti sopra indicati di gestione dei dati, Informativa ben visibile e Consenso.
- Un'app che registra la schermata dell'utente e non tratta questi dati come personali o sensibili e soggetti alle presenti norme.
- Un'app che rileva la posizione del dispositivo senza spiegarne in modo esauriente l'utilizzo e senza ottenere il consenso nel rispetto dei requisiti sopra indicati.
- Un'app che utilizza autorizzazioni limitate in background, ad esempio a scopi di monitoraggio, ricerca o marketing, senza spiegarne in modo esauriente l'utilizzo e senza ottenere il consenso nel rispetto dei requisiti sopra indicati.
- Un'app con un SDK che raccoglie dati utente personali e sensibili e che non li tratta come soggetti a queste norme relative ai dati utente e ai requisiti di consenso e visibilità dell'informativa, accesso e trattamento dei dati (tra cui vendita non consentita).

Fai riferimento a questo articolo per maggiori informazioni sul requisito di consenso e visibilità dell'informativa.

Limitazioni relative all'accesso a dati personali e sensibili

Oltre ai requisiti precedenti, esistono requisiti relativi ad attività specifiche che vengono riportati nella tabella qui sotto.

Attività	Requisito
L'app gestisce informazioni finanziarie, dati di pagamento o codici di identificazione ufficiali	L'app non deve mai rendere pubblici eventuali dati utente personali e sensibili relativi ad attività finanziarie o di pagamento oppure codici di identificazione ufficiali.
L'app gestisce dati della rubrica o informazioni di contatto non di pubblico dominio	Non è consentita la pubblicazione o la divulgazione non autorizzata di contatti non di pubblico dominio.
L'app contiene funzionalità di sicurezza o antivirus, ad esempio funzioni antivirus, antimalware o relative alla sicurezza	L'app deve pubblicare norme sulla privacy che, insieme a eventuali informative in-app, spieghino quali dati utente vengono raccolti e trasmessi nell'app, come vengono utilizzati e con chi vengono condivisi.
L'app è rivolta a bambini e ragazzi	L'app non deve includere un SDK non approvato per l'utilizzo nei servizi rivolti ai minori. Visita la pagina Progettare app per bambini e famiglie per leggere il testo completo delle norme e i requisiti.
L'app raccoglie o collega identificatori di dispositivi persistenti (ad esempio MEI, IMSI, numero di serie della SIM e così via)	Gli identificatori dei dispositivi persistenti non possono essere collegati ad altri dati utente personali e sensibili o a identificatori dei dispositivi reimpostabili, se non per le seguenti finalità: • servizi di telefonia collegati a un'identità SIM (ad esempio chiamate Wi-Fi collegate all'account di un operatore); e • app di gestione di dispositivi aziendali, utilizzando la modalità proprietario del dispositivo. Questi utilizzi devono essere comunicati in posizione ben visibile, come specificato nelle norme relative ai dati utente.

	Consulta questa risorsa per scoprire identificatori univoci alternativi. Leggi le norme relative agli annunci per avere ulteriori indicazioni relative all'ID pubblicità di Android.

Sezione Sicurezza dei dati

Tutti gli sviluppatori sono tenuti a compilare in modo chiaro e preciso una sezione Sicurezza dei dati per ogni app, fornendo spiegazioni dettagliate in merito alla raccolta, all'utilizzo e alla condivisione dei dati utente. Lo sviluppatore è responsabile dell'esattezza dell'etichetta e di mantenere aggiornate queste informazioni. Ove pertinente, la sezione deve essere conforme alle informative presenti nelle norme sulla privacy dell'app.

Leggi questo articolo per ulteriori informazioni sulla compilazione della sezione Sicurezza dei dati.

Norme sulla privacy

Per tutte le app è necessario pubblicare le norme sulla privacy inserendo un link nel relativo campo in Play Console e tramite un link o un testo all'interno dell'app stessa. Le norme sulla privacy, insieme a eventuali informative in-app, devono spiegare in modo esauriente in che modo l'app accede ai dati utente e li raccoglie, utilizza e condivide, intendendosi per dati utente tutti i dati, non soltanto quelli indicati nella sezione Sicurezza dei dati. È necessario includere:

- Informazioni sullo sviluppatore e un punto di contatto per la privacy oppure un meccanismo per inviare richieste di informazioni.
- La comunicazione dei tipi di dati utente personali e sensibili a cui l'app accede e che raccoglie, utilizza e condivide, nonché i soggetti con cui vengono eventualmente condivisi dati utente personali o sensibili.
- Procedure sicure di trattamento dei dati utente personali e sensibili.
- Le norme dello sviluppatore relative alla conservazione e all'eliminazione dei dati.
- Una chiara indicazione che si tratta di norme sulla privacy (ad esempio inserendo "norme sulla privacy" nel titolo).

Nelle norme sulla privacy deve essere indicata l'entità (ad esempio lo sviluppatore o la società) citata nella scheda del Google Play Store dell'app oppure deve essere specificato il nome dell'app. È necessario inviare le norme sulla privacy anche per le app che non accedono a dati utente personali e sensibili.

Assicurati che le norme sulla privacy siano disponibili su un URL attivo, pubblicamente accessibile e al di fuori di recinti virtuali (non PDF) e che non possano essere modificate.

Requisiti per l'eliminazione degli account

Se le tue app consentono agli utenti di creare un account dall'interno dell'app, devi anche consentire agli utenti di richiederne la cancellazione. Gli utenti devono disporre di un'opzione ben visibile per avviare l'eliminazione del loro account dall'app (ad esempio, visitando il tuo sito web). È necessario inserire un link a questa risorsa web nel campo dell'URL designato in Play Console.

Quando elimini un account dell'app sulla base di una richiesta di un utente, devi eliminare anche i dati utente associati a quell'account. Disattivare, disabilitare o bloccare temporaneamente l'account dell'app non equivale a eliminarlo. Se devi conservare determinati dati per motivi legittimi quali sicurezza, prevenzione delle frodi o conformità normativa, devi informare chiaramente gli utenti in merito alle tue pratiche di conservazione dei dati (ad esempio, nelle norme sulla privacy).

Per ulteriori informazioni sui requisiti relativi alle norme inerenti all'eliminazione degli account, consulta questo articolo del Centro assistenza. Per ulteriori informazioni sull'aggiornamento del modulo Sicurezza dei dati, consulta questo articolo.

Utilizzo dell'ID impostato per un insieme di app

Su Android verrà introdotto un nuovo ID per supportare i casi d'uso essenziali, ad esempio l'analisi e la prevenzione di attività fraudolente. Di seguito sono riportati i termini per l'utilizzo dell'ID.

- **Utilizzo.** L'ID set di app non deve essere usato per la personalizzazione e la valutazione degli annunci.
- **Associazione con informazioni che consentono l'identificazione personale o altri identificatori.** L'ID set di app non può essere collegato ad alcun identificatore Android (ad esempio AAID) o ad alcun dato personale e sensibile per finalità pubblicitarie.
- **Trasparenza e consenso.** La raccolta e l'utilizzo dell'ID set di app e l'impegno a rispettare i presenti termini devono essere comunicati agli utenti tramite un'Informativa sulla privacy legalmente adeguata che includa le tue norme sulla privacy. Devi ottenere il consenso legalmente valido degli utenti dove richiesto. Per ulteriori informazioni sui nostri standard relativi alla privacy, consulta le norme relative ai dati utente .

UE-U.S., Privacy Shield (scudo per la privacy) svizzero

Qualora tu acceda, utilizzi o elabori informazioni personali rese disponibili da Google che identificano un individuo in modo diretto o indiretto e provengono dall'Unione Europea o dalla Svizzera ("Informazioni personali dell'UE"), devi:

- Rispettare tutte le leggi, le direttive, i regolamenti e le norme vigenti in materia di privacy nonché di sicurezza e protezione dei dati;
- Utilizzare, elaborare le Informazioni personali dell'UE o accedervi solo per scopi conformi al consenso rilasciato dalla persona cui tali informazioni fanno riferimento;
- Implementare le misure organizzative e tecniche appropriate per proteggere le Informazioni personali dell'UE da perdita, uso improprio, accesso non autorizzato o illegale, divulgazione, alterazione e distruzione; e inoltre
- Fornire un livello di protezione pari a quello richiesto dai Principi del Privacy Shield (scudo per la privacy) .

Devi monitorare regolarmente il rispetto di queste condizioni. Se in qualsiasi momento non potessi rispettare queste condizioni (o se esiste un rischio elevato che tu possa non rispettarle), devi informarci immediatamente inviando un'email all'indirizzo data-protection-office@google.com e interrompere subito l'elaborazione delle Informazioni personali dell'UE o adottare misure ragionevoli e appropriate per ripristinare un adeguato livello di protezione.

Dal 16 luglio 2020, Google non si basa più sull'EU-U.S. Privacy Shield (scudo UE-USA per la privacy) per trasferire dati personali dallo Spazio economico europeo o dal Regno Unito negli Stati Uniti. (Ulteriori informazioni.) Per ulteriori informazioni, consulta la sezione 9 del Contratto di distribuzione per gli sviluppatori.

Autorizzazioni e API che accedono a informazioni sensibili

Le richieste di autorizzazioni e le API che accedono a informazioni sensibili dovrebbero essere sensate per gli utenti. Puoi richiedere solo le autorizzazioni e le API che accedono a informazioni sensibili necessarie per implementare funzionalità o servizi esistenti della tua app che vengono promossi nella scheda di Google Play. Non puoi utilizzare le autorizzazioni o le API che accedono a informazioni sensibili che consentono l'accesso ai dati dell'utente o del dispositivo per funzionalità o scopi non dichiarati, non implementati o non consentiti. I dati personali o sensibili accessibili tramite le autorizzazioni o le API che hanno accesso a informazioni sensibili non possono mai essere venduti né condivisi con lo scopo di facilitare la vendita.

Richiedi autorizzazioni e API che accedono a informazioni sensibili per accedere ai dati nel contesto (tramite richieste incrementali), in modo che gli utenti capiscano perché la tua app richiede l'autorizzazione. Devi utilizzare i dati solo per gli scopi a cui l'utente ha acconsentito. Se in un secondo

momento vuoi utilizzare i dati per altri scopi, devi fare richiesta agli utenti e accertarti che prestino consenso esplicito agli usi aggiuntivi.

Autorizzazioni limitate

In aggiunta a quanto sopra, le autorizzazioni limitate sono autorizzazioni definite come Pericolose , Speciali , Firma o come documentato di seguito. Queste autorizzazioni sono soggette alle restrizioni e ai requisiti aggiuntivi riportati di seguito:

- I dati degli utenti o dei dispositivi accessibili tramite Autorizzazioni limitate sono considerati dati utente personali e sensibili. Si applicano i requisiti delle norme relative ai dati utente .
- Se gli utenti rifiutano una richiesta di Autorizzazione limitata, devi rispettare la loro decisione. Gli utenti non possono essere manipolati o forzati a concedere autorizzazioni non fondamentali. Devi compiere un ragionevole sforzo per supportare gli utenti che non concedono l'accesso ad autorizzazioni sensibili, ad esempio consentendo loro di inserire manualmente un numero di telefono se hanno limitato l'accesso ai Registri chiamate.
- L'utilizzo di autorizzazioni in violazione delle norme relative ai malware di Google Play (tra cui Abuso di privilegio elevato) è espressamente vietato.

Alcune Autorizzazioni limitate potrebbero essere soggette a requisiti aggiuntivi, come descritto di seguito. L'obiettivo di queste restrizioni è tutelare la privacy degli utenti. Potremo concedere limitate eccezioni ai requisiti che seguono in rari casi in cui le app forniscano una funzionalità molto interessante o fondamentale e non esistano metodi alternativi per fornire tale funzionalità. Le eccezioni vengono valutate in base al potenziale impatto sulla privacy o sulla sicurezza degli utenti.

Autorizzazioni SMS e Registro chiamate

Le Autorizzazioni SMS e Registro chiamate sono considerate dati utente personali e sensibili soggetti alle norme relative a Informazioni personali e sensibili e alle seguenti restrizioni:

Autorizzazione limitata	Requisito
Gruppo di autorizzazioni Registro chiamate (ad esempio READ_CALL_LOG, WRITE_CALL_LOG, PROCESS_OUTGOING_CALLS)	Deve essere registrato e attivo come gestore predefinito del telefono o dell'assistente sul dispositivo.
Gruppo di autorizzazioni SMS (ad esempio, READ_SMS, SEND_SMS, WRITE_SMS, RECEIVE_SMS, RECEIVE_WAP_PUSH, RECEIVE_MMS)	Deve essere registrato e attivo come gestore predefinito di SMS o dell'assistente sul dispositivo.

Le app prive di funzionalità di gestore predefinito di SMS, telefono o assistente non possono dichiarare l'uso di queste autorizzazioni nel file manifest, incluso testo segnaposto. Inoltre, le app devono essere registrate attivamente come gestore predefinito di SMS, telefono o assistente prima di chiedere agli utenti di accettare le autorizzazioni di cui sopra e devono interrompere immediatamente l'utilizzo dell'autorizzazione qualora non siano più il gestore predefinito. Le eccezioni e gli usi consentiti sono disponibili in questa pagina del Centro assistenza .

Le app possono utilizzare l'autorizzazione (e tutti i dati da questa derivati) solo per fornire la funzionalità principale e approvata dell'app. La funzionalità principale è definita come lo scopo primario dell'app e può comprendere un insieme di funzionalità di base, che devono essere tutte documentate e promosse in evidenza nella descrizione dell'app. Senza la funzionalità o le funzionalità di base, l'app non funziona o è inutilizzabile. Il trasferimento, la condivisione o l'uso autorizzato mediante licenza di questi dati deve avvenire solo ed esclusivamente allo scopo di fornire funzionalità o servizi fondamentali all'interno dell'app e il loro uso non deve mai essere esteso a nessun altro scopo (ad esempio per migliorare altre app o servizi, per scopi pubblicitari o di marketing). Non è possibile utilizzare metodi alternativi (incluse altre autorizzazioni, API o fonti di terze parti) per ricavare i dati attribuiti alle autorizzazioni relative al registro chiamate o agli SMS.

Autorizzazioni di accesso alla posizione

La posizione del dispositivo è considerata un dato utente personale e sensibile soggetto alle norme relative alle informazioni personali e sensibili, alle norme relative alla posizione in background e ai seguenti requisiti:

- Le app non possono accedere ai dati protetti dalle autorizzazioni di accesso alla posizione (ad esempio, ACCESS_FINE_LOCATION, ACCESS_COARSE_LOCATION, ACCESS_BACKGROUND_LOCATION) quando non sono più necessari per offrire le funzionalità o i servizi inclusi nell'app.
- Lo sviluppatore non deve mai richiedere agli utenti le autorizzazioni di accesso alla posizione esclusivamente a scopi pubblicitari o di analisi. Le app che estendono l'utilizzo autorizzato di questi dati per la pubblicazione di annunci devono essere conformi alle nostre Norme relative agli annunci.
- Le app devono richiedere l'ambito minimo necessario (ad esempio, generico anziché specifico e in primo piano anziché in background) per fornire la funzionalità o il servizio corrente che richiede la posizione; inoltre, per gli utenti deve essere ragionevolmente prevedibile che la funzionalità o il servizio richieda il livello di posizione richiesto. Ad esempio, potremo rifiutare eventuali app che richiedano la posizione in background o accedano a questa senza una giustificazione convincente.
- La posizione in background può essere utilizzata soltanto per fornire funzionalità utili all'utente e attinenti alla funzionalità di base dell'app.

Le app possono accedere alla posizione usando l'autorizzazione di accesso al servizio in primo piano (che prevede per l'app soltanto l'accesso in primo piano, ad esempio "durante l'uso") se l'uso:

- È stato iniziato come continuazione di un'azione avviata dall'utente nell'app e inoltre
- Cessa immediatamente dopo che il caso d'uso previsto dell'azione avviata dall'utente viene completato dall'applicazione.

Le app progettate specificatamente per bambini e ragazzi devono essere conformi alle norme del programma Per la famiglia.

Per ulteriori informazioni sui requisiti delle norme, leggi questo articolo del Centro assistenza.

Autorizzazione di accesso a tutti i file

I file e gli attributi di directory sul dispositivo di un utente sono considerati dati utente personali e sensibili soggetti alle norme relative a Informazioni personali e sensibili e ai seguenti requisiti:

- Le app devono richiedere l'accesso solo allo spazio di archiviazione del dispositivo essenziale per il loro funzionamento e non possono richiedere l'accesso allo spazio di archiviazione per conto di terze parti per scopi non correlati alla funzionalità critica per gli utenti.
- I dispositivi Android su cui è installato R o versioni successive richiedono l'autorizzazione MANAGE_EXTERNAL_STORAGE per gestire l'accesso nell'archivio condiviso. Tutte le app destinate a R e che richiedono accesso completo all'archivio condiviso ("Accesso a tutti i file") devono superare una revisione di accesso appropriata prima della pubblicazione. Le app autorizzate a utilizzare questa autorizzazione devono chiedere chiaramente agli utenti di abilitare "Accesso a tutti i file" nelle impostazioni "Accesso speciale per le app". Ulteriori informazioni sui requisiti di R sono disponibili in questo articolo del Centro assistenza.

Autorizzazione di visibilità dei pacchetti (app)

L'inventario delle app installate a cui vengono inviate query da un dispositivo è considerato un dato utente personale e sensibile soggetto alle norme relative a informazioni personali e sensibili e ai seguenti requisiti:

Le app che hanno come scopo principale l'avvio, la ricerca o l'interoperabilità con altre app installate sul dispositivo possono ottenere visibilità, in conformità al relativo ambito, sulle altre app installate sul

dispositivo secondo le modalità descritte di seguito:

- **Ampia visibilità delle app.** Per "ampia visibilità" si intende la capacità di un'app di avere una visibilità estesa (o "ampia") rispetto alle app installate ("pacchetti") su un dispositivo.
  - Per le app destinate al livello API 30 o successivo , l'ampia visibilità sulle app installate tramite l'autorizzazione QUERY_ALL_PACKAGES è limitata a casi d'uso specifici in cui, per il corretto funzionamento dell'app, sono necessari il riconoscimento di e/o l'interoperabilità con tutte le app sul dispositivo.
    - Non è possibile usare l'autorizzazione QUERY_ALL_PACKAGES se l'app è in grado di funzionare con una dichiarazione di visibilità dei pacchetti con ambito più mirato , ad esempio inviando query a pacchetti specifici e interagendo con questi, evitando la richiesta di ampia visibilità.
  - Anche il ricorso a metodi alternativi per avvicinarsi al livello di ampia visibilità associato all'autorizzazione QUERY_ALL_PACKAGES è limitato alla funzionalità principale dell'app rivolta agli utenti e all'interoperabilità con qualsiasi app rilevata tramite tali metodi.
  - Consulta questo articolo del Centro assistenza relativo ai casi d'uso consentiti per l'autorizzazione QUERY_ALL_PACKAGES.
- **Visibilità limitata delle app.** Per "visibilità limitata" si intende una situazione in cui un'app riduce al minimo l'accesso ai dati inviando query per app specifiche tramite metodi più mirati, anziché "ampi", ad esempio inviando query per app specifiche che soddisfano la dichiarazione del file manifest dell'app che esegue la query. Puoi usare questo metodo per inviare query per app nei casi in cui la tua app includa funzionalità conformi alle norme di interazione con tali app o di gestione di queste.
- La visibilità sull'inventario delle app installate su un dispositivo deve essere direttamente correlata allo scopo principale o alla funzionalità principale a cui gli utenti hanno accesso all'interno dell'app.

I dati dell'inventario di app oggetto di query da parte di app distribuite su Google Play non possono mai essere venduti né condivisi a fini di analisi o di monetizzazione degli annunci.

API Accessibility

Non è possibile usare l'API Accessibility per:

- modificare le impostazioni degli utenti senza la loro autorizzazione o impedire agli utenti di disattivare o disinstallare app o servizi, a meno che non venga fornita autorizzazione da un genitore o tutore tramite un'app per il controllo genitori oppure da amministratori autorizzati tramite software di gestione aziendale;
- aggirare le notifiche e i controlli per la privacy integrati in Android oppure
- cambiare l'interfaccia utente o usarla in modo ingannevole o secondo modalità che violano le norme per gli sviluppatori di Google Play.

L'API Accessibility non è pensata e non può essere richiesta per la registrazione dell'audio delle chiamate da remoto.

L'uso dell'API Accessibility deve essere documentato nella scheda di Google Play.

Linee guida per IsAccessibilityTool

Le app con una funzionalità di base pensata per supportare direttamente le persone con disabilità possono essere debitamente e pubblicamente designate come app di accessibilità utilizzando **IsAccessibilityTool**.

Le app non idonee all'uso di **IsAccessibilityTool** non possono usare questa designazione e devono rispettare i requisiti relativi al consenso e alla visibilità dell'informativa indicati nelle norme relative ai dati utente , in quanto la funzionalità collegata all'accessibilità non è evidente per l'utente. Per ulteriori informazioni, leggi l'articolo del Centro assistenza Usare l'API AccessibilityService .

Quando possibile, le app devono usare API e autorizzazioni con ambito più limitato al posto dell'API Accessibility per ottenere la funzionalità desiderata.

Autorizzazione Richiesta di pacchetti di installazione

L'autorizzazione REQUEST_INSTALL_PACKAGES consente a un'applicazione di richiedere l'installazione di pacchetti dell'app. Per usare questa autorizzazione, la funzionalità di base dell'app deve includere:

- Invio o ricezione di pacchetti dell'app; e
- Attivazione dell'installazione dei pacchetti dell'app avviata dall'utente.

Le funzionalità consentite includono:

- Navigazione o ricerca sul web
- Servizi di comunicazione che supportano gli allegati
- Condivisione, trasferimento o gestione di file
- Gestione di dispositivi aziendali
- Backup e ripristino
- Migrazione dispositivi/trasferimento telefono
- App companion per sincronizzare il telefono a dispositivi indossabili o IoT (ad esempio, smartwatch o smart TV).

La funzionalità di base è lo scopo principale dell'app. La funzionalità di base e le eventuali funzionalità principali che la costituiscono devono essere tutte documentate e dichiarate in modo ben visibile nella descrizione dell'app.

Non è possibile usare l'autorizzazione REQUEST_INSTALL_PACKAGES per eseguire aggiornamenti automatici o modifiche o per creare bundle di altri APK nel file di asset, se non per finalità di gestione dei dispositivi. Tutti gli aggiornamenti o le installazioni di pacchetti devono avvenire in conformità con le norme relative all'utilizzo illecito di dispositivi e reti di Google Play, nonché essere avviati e gestiti dall'utente.

Autorizzazioni di Connessione Salute di Android

Connessione Salute è una piattaforma Android che consente alle app per la salute e l'attività fisica di archiviare e condividere gli stessi dati sul dispositivo all'interno di un ecosistema unificato. Offre inoltre agli utenti un unico posto per controllare quali app possono leggere e scrivere dati relativi a salute e attività fisica. Connessione Salute supporta la lettura e la scrittura di diversi tipi di dati , dai passi alla temperatura corporea.

I dati a cui accedi tramite le autorizzazioni di Connessione Salute sono considerati dati utente personali e sensibili soggetti alle norme relative ai dati utente. Se la tua app è classificata come un'app per la salute o ha funzionalità correlate alla salute e accede a dati sanitari, inclusi i dati di Connessione Salute, deve anche rispettare le norme relative alle app per la salute.

Per informazioni su come iniziare a usare Connessione Salute, consulta questa guida per gli sviluppatori Android . Per richiedere l'accesso ai tipi di dati di Connessione Salute, consulta questa pagina.

Le app distribuite tramite Google Play devono soddisfare i seguenti requisiti delle norme per poter leggere e/o scrivere dati in Connessione Salute.

Accesso e uso appropriati di Connessione Salute

Connessione Salute può essere usata esclusivamente nel rispetto delle norme e dei termini e condizioni vigenti e per i casi d'uso approvati, come previsto dalle presenti norme. Questo significa che puoi richiedere l'accesso alle autorizzazioni solo se la tua applicazione o il tuo servizio soddisfa uno dei casi d'uso approvati.

I casi d'uso approvati includono: attività fisica e benessere, premi, allenamento, benessere aziendale, assistenza medica, ricerca medica e giochi. Le applicazioni a cui è concesso l'accesso a tali autorizzazioni non possono estenderne l'utilizzo a finalità non comunicate o non consentite.

Solo le applicazioni o i servizi con una o più funzionalità progettate con lo scopo principale di andare a vantaggio di salute e attività fisica degli utenti possono richiedere l'accesso alle autorizzazioni di Connessione Salute. Sono inclusi:

- Le applicazioni o i servizi che consentono agli utenti di **registrare con regolarità, riportare, monitorare e/o analizzare direttamente** l'attività fisica, il sonno, il benessere mentale, l'alimentazione, le misurazioni relative allo stato di salute, le descrizioni fisiche e/o altre descrizioni o misurazioni relative alla salute o all'attività fisica.
- Le applicazioni o i servizi che consentono agli utenti di **archiviare sullo smartphone e/o sul dispositivo indossabile l'attività fisica, il sonno, il benessere mentale, l'alimentazione, le misurazioni relative allo stato di salute, le descrizioni fisiche** e/o altre descrizioni o misurazioni relative alla salute o all'attività fisica e condividere i dati con altre app sul dispositivo che soddisfano i presenti casi d'uso.

L'accesso a Connessione Salute non può essere utilizzato in violazione delle presenti norme o di altri termini e condizioni o norme di Connessione Salute vigenti. Ciò include le finalità indicate di seguito:

- Non utilizzare Connessione Salute per lo sviluppo di (o per l'integrazione in) applicazioni, ambienti o attività in cui ci si può ragionevolmente attendere che l'uso o il malfunzionamento di Connessione Salute possa causare morte, lesioni personali o danni ambientali o materiali (ad esempio per la creazione o il funzionamento di impianti nucleari, controllo del traffico aereo, sistemi salvavita o armi).
- Non accedere a dati ottenuti mediante Connessione Salute usando app headless. Le app devono mostrare un'icona facilmente identificabile nella barra delle applicazioni, nelle impostazioni delle app sul dispositivo, nelle icone di notifica e così via.
- Non utilizzare Connessione Salute con app che sincronizzano dati tra dispositivi o piattaforme non compatibili.
- Non utilizzare Connessione Salute per collegarti ad applicazioni, servizi o funzionalità destinati esclusivamente ai bambini.
- Adotta misure ragionevoli e appropriate per proteggere tutti i sistemi o le applicazioni che fanno uso di Connessione Salute da accesso, utilizzo, distruzione, perdita, modifica o divulgazione non autorizzati o illegali.

È inoltre tua responsabilità garantire la conformità con qualsiasi requisito normativo o legale eventualmente vigente in base all'uso da te previsto di Connessione Salute e degli eventuali dati contenuti nell'app. Google, fatto salvo quanto espressamente indicato sulle etichette o nelle informazioni fornite da Google stessa per prodotti o servizi Google specifici, non raccomanda l'uso, né garantisce l'accuratezza dei dati contenuti in Connessione Salute per alcun impiego o scopo e, in particolare, per usi connessi alla ricerca, alla salute o medicali. Google non si assume alcuna responsabilità associata all'uso dei dati ottenuti mediante Connessione Salute.

Uso limitato

Quando si utilizza Connessione Salute, l'accesso ai dati e il relativo uso devono ottemperare a limitazioni specifiche:

- L'uso dei dati dovrebbe essere limitato alla fornitura o al miglioramento del caso d'uso appropriato o delle funzionalità visibili nell'interfaccia utente dell'applicazione.
- I dati dell'utente possono essere trasferiti a terze parti solo con il suo consenso esplicito: per finalità di sicurezza (ad esempio, per indagare su abusi), per rispettare leggi o regolamenti vigenti o nell'ambito di fusioni/acquisizioni.
- L'accesso ai dati utente da parte di persone è limitato salvo l'ottenimento del consenso esplicito dell'utente, a fini di sicurezza, di conformità con le leggi o quando i dati sono aggregati per operazioni interne come da requisiti legali.
- È proibito qualsiasi altro trasferimento, uso o vendita dei dati di Connessione Salute, inclusi:

- Il trasferimento o la vendita di dati utente a terze parti, ad esempio piattaforme pubblicitarie, intermediari di dati o qualsiasi rivenditore di informazioni.
- Il trasferimento, la vendita o l'uso di dati utente per la pubblicazione di annunci, inclusa la pubblicità personalizzata o basata sugli interessi.
- Il trasferimento, la vendita o l'uso di dati utente per determinare l'affidabilità creditizia o per finalità di prestito.
- Il trasferimento, la vendita o l'uso di dati utente con qualsiasi prodotto o servizio che possa essere considerato un dispositivo medico ai sensi della Sezione 201(h) del Federal Food Drug and Cosmetic Act qualora i dati utente vengano usati dal dispositivo medico per l'esecuzione della sua funzionalità regolamentata.
- Il trasferimento, la vendita o l'uso di dati utente per qualsiasi scopo o in qualsiasi modalità che coinvolga dati sanitari protetti (come definiti dalla normativa HIPAA) a meno che tu non disponga della preventiva autorizzazione scritta di Google per tale uso.

Ambito minimo

Devi solo richiedere l'accesso alle autorizzazioni necessarie per implementare le funzionalità o i servizi del tuo prodotto. Tali richieste di accesso dovrebbero essere specifiche e limitate ai dati necessari.

Trasparenza e accuratezza di comunicazioni e controllo

Connessione Salute gestisce i dati relativi a salute e attività fisica, comprese le informazioni sensibili, e richiede che tutte le applicazioni dispongano di norme sulla privacy complete. Le norme sulla privacy devono comunicare in maniera trasparente il modo in cui l'app raccoglie, utilizza e condivide i dati utente. Oltre ai requisiti legali, gli sviluppatori devono includere le seguenti informazioni nelle norme sulla privacy:

- Descrivere accuratamente l'identità dell'app, indicando i dati a cui accede e il relativo collegamento a consigli o funzionalità in evidenza dell'app.
- Pratiche di conservazione ed eliminazione dei dati.
- Procedure di trattamento dei dati. Ad esempio, la trasmissione dei dati mediante metodi moderni di crittografia (ad esempio, tramite HTTPS).

Gestione sicura dei dati

Devi gestire tutti i dati utente in sicurezza. Adotta misure ragionevoli e appropriate per proteggere tutti i sistemi o le applicazioni che fanno uso di Connessione Salute da accesso, utilizzo, distruzione, perdita, modifica o divulgazione non autorizzati o illegali.

Le misure di sicurezza consigliate includono la messa e il mantenimento in opera di un sistema di gestione della sicurezza informatica come indicato nella norma ISO/IEC 27001 e la garanzia che l'applicazione o il servizio web sia affidabile e privo di problemi di sicurezza comuni quali quelli indicati nelle OWASP Top 10.

In base all'API a cui si esegue l'accesso e al numero di utenti, richiederemo che l'applicazione o il servizio siano sottoposti a valutazioni di sicurezza periodiche e ottengano una lettera di valutazione di una terza parte designata qualora il prodotto trasferisca i dati fuori dal dispositivo dell'utente.

Per ulteriori informazioni sui requisiti delle app che si collegano a Connessione Salute, consulta questo articolo del Centro assistenza.

Servizio VPN

VpnService è una classe base che consente alle applicazioni di estendere e creare le proprie soluzioni VPN. Solo le app che utilizzano VpnService la cui funzionalità di base è una VPN possono creare un tunnel sicuro a livello di dispositivo verso un server remoto. Tra le eccezioni figurano le app che richiedono un server remoto per la funzionalità di base, ad esempio:

- App di gestione aziendale e per il controllo genitori.

- Monitoraggio dell'utilizzo di app.
- App per la sicurezza del dispositivo (come antivirus, gestione dei dispositivi mobili, firewall).
- Strumenti relativi alla rete (come l'accesso remoto).
- App di navigazione sul Web.
- App di operatori che richiedono l'uso della funzionalità VPN per fornire servizi di telefonia o connettività.

Non è possibile usare VpnService per:

- Raccogliere dati utente personali e sensibili senza un'informativa ben visibile e senza aver ottenuto il consenso.
- Reindirizzare o manipolare il traffico utente da altre app su un dispositivo a scopi di monetizzazione (ad esempio reindirizzare il traffico dagli annunci pubblicitari in un paese diverso da quello dell'utente).

Le app che usano VpnService devono:

- Documentare l'uso di VpnService nella scheda di Google Play; e
- Criptare i dati dal dispositivo al punto di arrivo del tunnel VPN; e
- Rispettare tutte le Norme del programma per gli sviluppatori , incluse le norme relative a frodi pubblicitarie , autorizzazioni e malware .

Autorizzazione Sveglia esatta

Verrà introdotta una nuova autorizzazione chiamata USE_EXACT_ALARM per concedere l'accesso alla funzionalità di sveglia esatta nelle app su Android 13 e versioni successive (Livello API target 33).

USE_EXACT_ALARM è un'autorizzazione limitata e le app devono dichiararla solo se la loro funzionalità di base supporta l'esigenza di una sveglia esatta. Le app che richiedono questa autorizzazione limitata sono soggette a verifica e quelle che non soddisfano i criteri delle norme di utilizzo accettabile non potranno essere pubblicate su Google Play.

Casi d'uso accettabili per l'utilizzo dell'autorizzazione Sveglia esatta

La tua app deve usare la funzionalità USE_EXACT_ALARM solo quando la funzionalità principale rivolta all'utente della tua app richiede azioni temporizzate in modo preciso, ad esempio:

- L'app è una sveglia o un timer.
- L'app è un calendario che mostra notifiche di eventi.

Se il tuo caso d'uso per la funzionalità di sveglia esatta non rientra tra quelli menzionati, dovresti valutare se esiste la possibilità di usare SCHEDULE_EXACT_ALARM in alternativa.

Per ulteriori informazioni sulla funzionalità di sveglia esatta, consulta queste indicazioni per gli sviluppatori .

Autorizzazione relativa agli intent a schermo intero

Per le app che hanno come target Android 14 (livello API target 34) e versioni successive, USE_FULL_SCREEN_INTENT è un'autorizzazione di accesso alle app speciale. . Alle app sarà consentito automaticamente l'utilizzo dell'autorizzazione USE_FULL_SCREEN_INTENT se la loro funzionalità di base rientra tra una delle seguenti categorie che richiedono notifiche ad alta priorità:

- Impostazione di una sveglia
- Ricezione di telefonate e videochiamate

Le app che richiedono questa autorizzazione sono soggette a verifica e a quelle che non soddisfano i suddetti criteri non sarà concessa automaticamente l'autorizzazione. In tal caso, le app devono richiedere l'autorizzazione all'utente per utilizzare USE_FULL_SCREEN_INTENT.

Ricorda **che** tutti gli utilizzi dell'autorizzazione USE_FULL_SCREEN_INTENT devono rispettare tutte le norme per gli sviluppatori di Google Play, incluse le nostre norme relative al software mobile indesiderato, all'utilizzo illecito di dispositivi e retie agli annunci. Le notifiche di intent a schermo intero non possono interferire con, interrompere, danneggiare o accedere al dispositivo dell'utente senza autorizzazione. Inoltre, le app non devono interferire con altre app o con l'usabilità del dispositivo.

Scopri di più sull'autorizzazione USE_FULL_SCREEN_INTENT nel nostro Centro assistenza.

Utilizzo illecito di dispositivi e reti

Sono vietate le app che accedono senza autorizzazione al dispositivo dell'utente, ad altri dispositivi o computer, server, reti, API (interfaccia di programmazione di un'applicazione) o servizi, inclusi, a titolo esemplificativo, altre app sul dispositivo, servizi di Google o la rete di un operatore autorizzato, o che li interrompono, danneggiano o ostacolano..

Le app su Google Play devono rispettare i requisiti di ottimizzazione del sistema Android predefiniti e documentati nelle Norme fondamentali sulla qualità delle app per Google Play .

Un'app distribuita tramite Google Play non può essere modificata, sostituita o aggiornata utilizzando metodi diversi dal meccanismo di aggiornamento di Google Play. Analogamente, un'app non può scaricare codice eseguibile (ad esempio file dex, JAR e .so) da una fonte diversa da Google Play. Questa limitazione non riguarda il codice che viene eseguito su una macchina virtuale o un interprete che danno accesso indiretto alle API Android (ad esempio JavaScript in un componente WebView o in un browser).

App o codice di terze parti (ad esempio SDK) con linguaggi interpretati (JavaScript, Python, Lua e così via) caricati in fase di runtime (ad esempio non inclusi nell'app) non devono consentire potenziali violazioni delle norme di Google Play.

È vietato il codice che introduce o sfrutta vulnerabilità di sicurezza. Consulta il Programma App Security Improvement per scoprire i problemi di sicurezza più recenti segnalati agli sviluppatori.

Di seguito sono riportati alcuni esempi di violazioni frequenti:

Esempi di violazioni comuni relative all'utilizzo illecito di dispositivi e reti:

- App che bloccano o interferiscono con un'altra app mostrando annunci.
- App che alterano il gameplay di altre app consentendo di barare.
- App che facilitano la compromissione di servizi, software o hardware, l'elusione di misure di sicurezza o che forniscono istruzioni a riguardo.
- App che utilizzano o accedono a un servizio o a un'API con modalità che costituiscono una violazione dei relativi termini di servizio.
- App che non sono idonee all'inserimento in lista consentita e che tentano di aggirare le misure di gestione dell'alimentazione di sistema .
- Le app che agevolano servizi proxy verso terzi sono consentite solo laddove questo sia lo scopo principale dell'app proposto all'utente.
- App o codice di terze parti (ad esempio, SDK) che scaricano codice eseguibile, ad esempio file dex o codice nativo, da una fonte diversa da Google Play.
- App che installano altre app su un dispositivo senza previo consenso dell'utente.
- App che agevolano o rimandano alla distribuzione o all'installazione di software dannoso.
- App o codice di terze parti (ad esempio SDK) contenenti un componente WebView con interfaccia JavaScript aggiunta che carica contenuti web non attendibili (ad esempio, URL http://) oppure URL non verificati derivanti da fonti non attendibili (ad esempio, URL derivanti da intent non attendibili).
- App che usano l'autorizzazione relativa agli intent a schermo intero per forzare l'interazione dell'utente con notifiche o annunci improvvisi.

Utilizzo del servizio in primo piano

L'autorizzazione del servizio in primo piano garantisce che i servizi in primo piano rivolti agli utenti siano utilizzati in modo appropriato. Per le app che hanno come target Android 14 e versioni successive, devi specificare un tipo di servizio in primo piano valido per ogni servizio in primo piano utilizzato nell'app e dichiarare la relativa autorizzazione appropriata per quel tipo. Ad esempio, se il caso d'uso della tua app richiede la geolocalizzazione sulla mappa, devi dichiarare l'autorizzazione FOREGROUND_SERVICE_LOCATION nel file manifest dell'app.

Le app possono dichiarare un'autorizzazione per i servizi in primo piano solo se l'utilizzo:

- fornisce una funzionalità vantaggiosa per l'utente e pertinente alla funzionalità di base dell'app
- viene avviato o può essere percepito dall'utente (ad esempio, l'audio di una canzone in riproduzione, la trasmissione di contenuti multimediali a un altro dispositivo, una notifica per l'utente chiara e precisa, la richiesta dell'utente di caricare una foto sul cloud)
- può essere risolto o interrotto dall'utente
- non può essere interrotto o differito dal sistema senza causare un'esperienza utente negativa o malfunzionamenti della funzionalità attesa dall'utente (ad esempio, una chiamata deve essere avviata immediatamente e non può essere differita dal sistema)
- dura solo il tempo necessario al completamento dell'attività

I seguenti casi d'uso dei servizi in primo piano sono esenti dai criteri di cui sopra:

- tipi di servizi in primo piano systemExempted o shortService
- tipo di servizio in primo piano dataSync solo quando si utilizzano le funzionalità Play Asset Delivery

L'utilizzo del servizio in primo piano è spiegato più approfonditamente in questa pagina.

User-Initiated Data Transfer Jobs

Le app sono autorizzate a utilizzare l'API User-Initiated Data Transfer Jobs solo se l'utilizzo:

- è avviato dall'utente;
- è volto all'attività di trasferimento di dati di rete;
- dura solo il tempo necessario al completamento del trasferimento di dati.

L'utilizzo delle API User-Initiated Data Transfer è spiegato più approfonditamente in questa pagina.

Requisiti di Flag Secure

FLAG_SECURE è un flag di visualizzazione dichiarato nel codice di un'app e indica che la sua UI contiene dati sensibili che devono essere limitati a una piattaforma sicura durante l'utilizzo dell'app. Questo flag è progettato per impedire che i dati vengano mostrati in screenshot o in visualizzazioni non sicure. Gli sviluppatori dichiarano questo flag quando i contenuti dell'app non devono essere trasmessi, visualizzati né altrimenti inviati al di fuori dell'app o del dispositivo dell'utente.

Per ragioni di sicurezza e privacy, tutte le app distribuite su Google Play devono rispettare la dichiarazione di FLAG_SECURE delle altre app. In altre parole, le app non devono agevolare o creare soluzioni alternative per bypassare le impostazioni di FLAG_SECURE in altre app.

Le app che si qualificano come Strumenti di accessibilità non sono tenute a rispettare questo requisito, purché non trasmettano, salvino o memorizzino nella cache contenuti protetti da FLAG_SECURE per l'accesso al di fuori del dispositivo dell'utente.

App che vengono eseguite in contenitori per Android sul dispositivo

Le app di contenitori per Android sul dispositivo offrono ambienti che simulano interamente o parzialmente porzioni di un sistema operativo Android. L'esperienza all'interno di questi ambienti potrebbe non riflettere la suite completa delle funzionalità di sicurezza Android , per questo motivo

gli sviluppatori possono scegliere di aggiungere un flag del manifest relativo all'ambiente sicuro per comunicare ai contenitori per Android sul dispositivo che non devono operare negli ambienti Android simulati.

Flag del manifest relativo all'ambiente sicuro

REQUIRE_SECURE_ENV è un flag che è possibile dichiarare nel file manifest di un'app per indicare che l'app in questione non deve essere eseguita in app di contenitori per Android sul dispositivo. Per ragioni di sicurezza e privacy, le app che forniscono contenitori per Android sul dispositivo devono rispettare tutte le app che dichiarano questo flag e:

- Rivedere i file manifest delle app che intendono caricare nel loro contenitore per Android sul dispositivo per questo flag.
- Non caricare le app che hanno dichiarato questo flag nel loro contenitore per Android sul dispositivo.
- Non funzionare da proxy intercettando o chiamando le API sul dispositivo in modo da sembrare installate nel contenitore.
- Non agevolare o creare soluzioni alternative per bypassare il flag (ad esempio, caricando una versione precedente di un'app per bypassare l'attuale flag dell'app REQUIRE_SECURE_ENV).

Puoi trovare ulteriori informazioni su queste norme nel nostro Centro assistenza.

Comportamento ingannevole

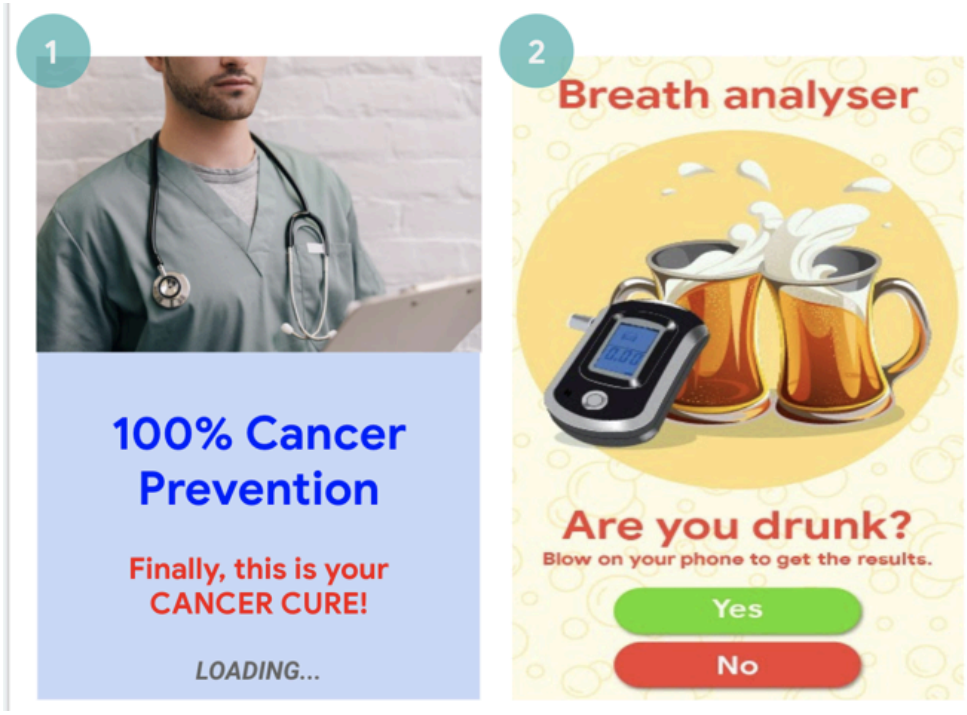
Sono vietate le app che cercano di ingannare gli utenti o di favorire comportamenti disonesti incluse, a titolo esemplificativo ma non esaustivo, tutte le app il cui funzionamento sia determinato essere impossibile. Le app devono contenere comunicazioni, descrizioni e immagini/video precisi relativi alla loro funzionalità in ogni parte dei metadati. Non devono cercare di imitare funzionalità e avvisi del sistema operativo o di altre app. Eventuali modifiche alle impostazioni del dispositivo non devono essere apportate all'insaputa e senza il consenso dell'utente e devono poter essere ripristinate dall'utente stesso.

Affermazioni ingannevoli

Non sono ammesse le app contenenti informazioni o dichiarazioni false o fuorvianti, neanche nella descrizione, nel titolo, nell'icona e negli screenshot.

Di seguito sono riportati alcuni esempi di violazioni frequenti:

- App contenenti rappresentazioni ingannevoli oppure descrizioni non precise e chiare in merito alla loro funzionalità:
  - Un'app contenente una descrizione e screenshot che suggeriscono che si tratta di un gioco di corse automobilistiche quando, in realtà, si tratta di un gioco di puzzle a blocchi per cui viene utilizzata l'immagine di un'auto.
  - Un'app presentata come un'app antivirus, ma che in realtà contiene soltanto una guida testuale che spiega come rimuovere i virus.
- App che dichiarano di avere funzionalità che non è possibile implementare, ad esempio app repellenti per gli insetti, anche se rappresentate come scherzi, falsi, prese in giro e così via.
- App classificate in modo errato inclusa, a titolo esemplificativo, la relativa classificazione o categoria.
- Contenuti manifestamente ingannevoli o falsi che potrebbero interferire con processi di voto oppure relativi ai risultati di elezioni.
- App che dichiarano falsamente di essere affiliate con enti governativi o di offrire o agevolare servizi governativi per i quali non sono debitamente autorizzate.
- App che dichiarano falsamente di essere le app ufficiali di un'entità riconosciuta. Titoli quali "App ufficiale di Justin Bieber" sono vietati senza le autorizzazioni o i diritti necessari.



(1) Questa app include dichiarazioni ingannevoli di tipo medico o sanitario (cura del cancro).
(2) Questa app dichiara di avere funzionalità che non è possibile implementare (uso dello smartphone come etilometro).

Modifiche ingannevoli alle impostazioni del dispositivo

Sono vietate le app che apportano modifiche alle impostazioni o alle funzionalità del dispositivo dell'utente al di fuori dell'app, all'insaputa e senza il consenso dell'utente. Le impostazioni e funzionalità del dispositivo includono: impostazioni del sistema e del browser, preferiti, scorciatoie, icone, widget e la presentazione di app nella schermata Home.

Sono inoltre vietate:

- App che modificano le impostazioni o funzionalità del dispositivo con il consenso dell'utente, ma con modalità che non consentono un facile ripristino.
- App o annunci che modificano le impostazioni o funzionalità del dispositivo come servizio per terze parti o per scopi pubblicitari.
- App che inducono con l'inganno gli utenti a rimuovere o disattivare app di terze parti oppure a modificare impostazioni o funzionalità del dispositivo.
- App che esortano o incoraggiano gli utenti a rimuovere o disattivare app di terze parti oppure a modificare impostazioni o funzionalità del dispositivo, se non nell'ambito di un servizio di sicurezza verificabile.

Favorire comportamenti disonesti

Non sono ammesse le app che aiutano gli utenti a ingannare altre persone o che sono in qualsiasi modo ingannevoli dal punto di vista funzionale incluse, a titolo esemplificativo, app che generano o favoriscono la generazione di carte d'identità, codici fiscali, passaporti, diplomi, carte di credito, conti bancari e patenti di guida. Le app devono contenere comunicazioni, titoli, descrizioni e immagini/video accurati in relazione alla loro funzionalità e/o ai loro contenuti e funzionare secondo le ragionevoli e precise aspettative dell'utente.

Il download di risorse aggiuntive delle app (ad esempio, relative a giochi) può avvenire solo quando tali risorse siano necessarie all'utilizzo dell'app da parte dell'utente. Le risorse scaricate devono essere conformi a tutte le norme di Google Play e, prima di iniziare il download, l'app dovrebbe informare gli utenti e mostrare in maniera chiara le dimensioni del download.

Le app indicate come "scherzo" o come create "per scopi di intrattenimento" (o altri sinonimi) non sono esenti dall'applicazione delle nostre norme.

Di seguito sono riportati alcuni esempi di violazioni frequenti:

- App che imitano altre app o siti web per indurre con l'inganno gli utenti a comunicare informazioni personali o dati di autenticazione.
- App che mostrano o presentano numeri telefonici, contatti, indirizzi o informazioni che consentono l'identificazione personale, reali o non verificati, di individui o entità non consenzienti.
- App con funzionalità principali diverse in base all'area geografica dell'utente, ai parametri del dispositivo o ad altri dati dipendenti dall'utente in cui tali differenze non vengono pubblicizzate in modo evidente per l'utente nella scheda dello Store.
- App che cambiano in modo significativo da una versione all'altra senza avvisare l'utente (ad esempio, sezione "novità") né aggiornare la scheda dello Store.
- App che tentano di modificare oppure offuscare il comportamento durante la revisione.
- App con download facilitati da Rete CDN (Content Delivery Network) che non informano l'utente e non specificano le dimensioni del download prima dello stesso.

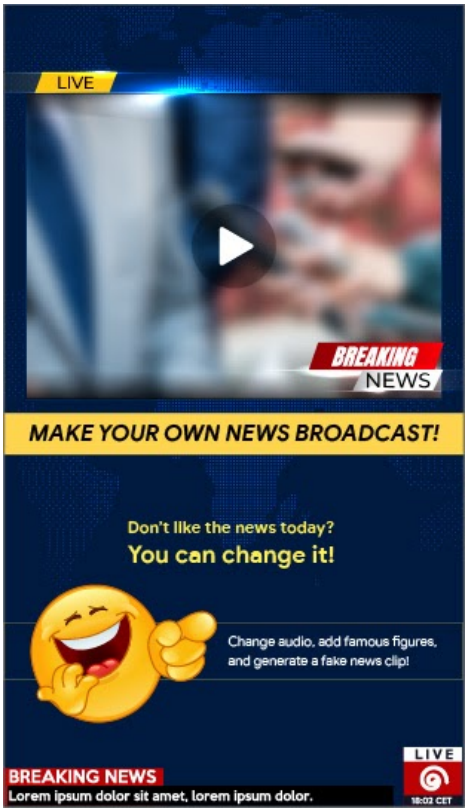
Contenuti multimediali manipolati

Sono vietate le app che promuovono o contribuiscono a creare informazioni o dichiarazioni false o fuorvianti trasmesse attraverso immagini, audio, video e/o testo. Sono vietate le app che vengano determinate promuovere o diffondere immagini, video e/o testo oggettivamente fuorvianti o ingannevoli, che potrebbero causare danni in relazione a un evento sensibile, a questioni politiche, a problemi sociali o altre questioni di pubblico interesse.

Le app che manipolano o alterano contenuti multimediali, al di là delle modifiche accettabili da un punto di vista editoriale allo scopo di migliorare qualità o chiarezza, devono visualizzare i contenuti alterati in modo evidente o con una filigrana, laddove all'utente medio possa non essere chiaro che tali contenuti sono stati alterati. Eccezioni possono essere contemplate nel caso di questioni di interesse pubblico oppure di satira o parodia evidenti.

Di seguito sono riportati alcuni esempi di violazioni frequenti:

- App che aggiungono un personaggio pubblico a una dimostrazione durante un evento politicamente sensibile.
- App che utilizzano personaggi pubblici o contenuti multimediali correlati a un evento sensibile per pubblicizzare la capacità di alterazione di contenuti multimediali all'interno della scheda dello Store di un'app.
- App che alterano clip multimediali per simulare un notiziario.



(1) Questa app fornisce funzionalità per alterare i clip multimediali per simulare un notiziario e aggiungere personaggi famosi o pubblici al clip senza watermark.

Trasparenza del comportamento

La funzionalità della tua app deve essere ragionevolmente chiara agli utenti; non includere nella tua app funzionalità nascoste, inattive o non provviste di documentazione. Non sono consentite tecniche per evitare i controlli delle app. Potrebbe essere obbligatorio fornire ulteriori dettagli sulle app per garantire la sicurezza degli utenti, l'integrità del sistema e la conformità alle norme.

Rappresentazione ingannevole

Sono vietati gli account sviluppatore e le app che:

- Assumono l'identità di persone o organizzazioni oppure che occultano o rappresentano in maniera ingannevole informazioni sulla propria proprietà o sul proprio scopo principale.
- Intraprendono attività coordinate allo scopo di ingannare gli utenti. Sono inclusi, a titolo esemplificativo ma non esaustivo, gli account sviluppatore o le app che travisano o nascondono il proprio paese di origine e che indirizzano contenuti a utenti di un altro paese.
- Si coordinano con altri siti, sviluppatori, app o account per occultare o rappresentare in maniera ingannevole l'identità dell'app o dello sviluppatore o altri dati personali, se i contenuti proposti sono relativi a politica, problemi sociali o questioni di interesse pubblico.

Norme di Google Play relative ai livelli API target

Per offrire agli utenti un'esperienza sicura e protetta, Google Play richiede i seguenti livelli API target per **tutte le app**:

Le nuove app e gli aggiornamenti delle app DEVONO avere come target un livello API Android che risalga al massimo a un anno prima del rilascio della più recente versione principale di Android. Per le nuove app e gli aggiornamenti delle app che non rispetteranno questo requisito non sarà possibile inviare app in Play Console.

Le app di Google Play esistenti che non sono aggiornate e che non avranno come target un livello API che risalga al massimo a due anni prima del rilascio della più recente versione principale di Android non saranno disponibili per i nuovi utenti con dispositivi su cui sono installate versioni più recenti del sistema operativo Android. Gli utenti che hanno già installato l'app da Google Play potranno continuare a trovarla, reinstallarla e usarla su qualsiasi versione del sistema operativo Android supportata dall'app.

Per consigli tecnici su come soddisfare il requisito relativo ai livelli API target, consulta la guida alla migrazione .

Per conoscere le eccezioni e le tempistiche esatte, leggi questo articolo del Centro assistenza .

Requisiti relativi all'SDK

Gli sviluppatori di app spesso si affidano a codice di terze parti (ad esempio, un SDK) per integrare funzionalità e servizi chiave per le loro app. Quando includi un SDK nella tua app, devi assicurarti che gli utenti siano al sicuro e che la tua app sia protetta da qualsiasi vulnerabilità. In questa sezione dimostriamo come alcuni dei nostri attuali requisiti di privacy e sicurezza si applichino al contesto degli SDK e siano pensati per aiutare gli sviluppatori a integrare in modo sicuro e protetto gli SDK nelle loro app.

Se includi un SDK nella tua app, hai la responsabilità di assicurarti che il codice e le pratiche di terze parti non facciano sì che la tua app violi le Norme del programma per gli sviluppatori di Google Play. È importante conoscere il modo in cui gli SDK dell'app gestiscono i dati utente e assicurarsi di sapere quali autorizzazioni utilizzano, quali dati raccolgono e perché. È bene ricordare che la raccolta e la gestione dei dati utente da parte di un SDK devono essere in linea con la norma relativa all'utilizzo di questi dati da parte dell'app.

Per assicurarti che l'uso di un SDK non violi i requisiti della norma, leggi e comprendi le seguenti norme nella loro interezza e prendi nota di alcuni dei requisiti esistenti relativi agli SDK riportati di seguito:

Norme relative ai dati utente

Devi assicurare la trasparenza in merito alla modalità di gestione dei dati utente (ad esempio le informazioni fornite da un utente o raccolte in relazione a un utente, incluse le informazioni del dispositivo). Ciò significa divulgare accesso, raccolta, utilizzo, trattamento e condivisione dei dati utente dalla tua app e limitare l'utilizzo dei dati agli scopi conformi alle norme dichiarati.

Se nell'app includi un codice di terze parti (ad esempio, un SDK), devi garantire che questo codice e le procedure di terze parti che rispettano i dati utente nella tua app siano conformi alle Norme del programma per gli sviluppatori di Google Play, che includono i requisiti relativi alle informative e all'utilizzo. Ad esempio, devi assicurarti che i tuoi provider di SDK non vendano dati utente personali e sensibili recuperati dalla tua app. Questo requisito si applica a prescindere se i dati utenti vengono trasferiti dopo essere stati inviati a un server o tramite l'incorporamento di un codice di terze parti nella tua app.

Dati utente personali e sensibili

- Devi limitare accesso, raccolta, utilizzo e condivisione di dati utente personali e sensibili acquisiti tramite l'app a funzionalità di app e servizi e scopi conformi alle norme ragionevolmente previste dall'utente come segue:
  - Le app che estendono l'utilizzo dei dati utente personali e sensibili per la pubblicazione di annunci devono essere conformi alle norme relative agli annunci di Google Play.
- Devi gestire tutti i dati utente personali e sensibili in sicurezza, compresa la loro trasmissione utilizzando metodi moderni di crittografia (ad esempio, tramite HTTPS).
- Devi utilizzare una richiesta di autorizzazioni di runtime ogni qual volta sia disponibile, prima di accedere ai dati controllati tramite autorizzazioni Android.

Vendita di dati utente personali e sensibili

Non devi vendere dati utente personali e sensibili.

- Per "vendita" si intende lo scambio o il trasferimento di dati utente personali e sensibili a una terza parte per un corrispettivo monetario.
  - Non viene inteso come vendita il trasferimento avviato dagli utenti di dati utente personali e sensibili, ad esempio quando un utente usa una funzionalità dell'app per trasferire un file a una terza parte o quando sceglie di usare un'app di studio per scopi dedicati.

Requisiti di consenso e informativa ben visibile

Nei casi in cui accesso, raccolta, utilizzo o condivisione di dati utente personali e sensibili da parte della tua app non rientrino nelle ragionevoli previsioni dell'utente in merito al prodotto o alla funzionalità in questione devi rispettare i requisiti di consenso e visibilità dell'informativa delle norme relative ai dati utente.

Se la tua app integra un codice di terze parti (ad esempio, un SDK) progettato per raccogliere dati utente personali e sensibili per impostazione predefinita, entro 2 settimane dalla ricezione di una richiesta di Google Play (o, se la richiesta di Google Play prevede un periodo di tempo maggiore, entro questo periodo) devi fornire prove sufficienti a dimostrare che la tua app soddisfa i requisiti di consenso e visibilità dell'informativa di questa norma, ad esempio in relazione ad accesso, raccolta, utilizzo o condivisione dei dati tramite il codice di terze parti.

Assicurati che l'uso di codice di terze parti (ad esempio, un SDK) non faccia sì che la tua app violi le norme relative ai dati utente.

Fai riferimento a questo articolo del Centro assistenza per ulteriori informazioni sul requisito di consenso e visibilità dell'informativa.

Esempi di violazioni causate dagli SDK

- Un'app con un SDK che raccoglie dati utente personali e sensibili e che non li tratta come soggetti a queste norme relative ai dati utente e ai requisiti di consenso e visibilità dell'informativa, accesso e trattamento dei dati (tra cui vendita non consentita).
- Un'app integra un SDK che raccoglie dati utente personali e sensibili per impostazione predefinita, in violazione dei requisiti di queste norme relativi al consenso dell'utente e all'informativa ben visibile.
- Un'app con un SDK che dichiara di raccogliere dati utente personali e sensibili solo per fornire all'app funzionalità di lotta alle frodi e agli abusi, mentre l'SDK condivide anche i dati raccolti con terze parti per pubblicità o analisi.
- Un'app include un SDK che trasmette le informazioni sui pacchetti installati dagli utenti senza rispettare le linee guida relative all'informativa ben visibile e/o le linee guida sulle norme sulla privacy.
  - Consulta anche le norme relative al software mobile indesiderato.

Ulteriori requisiti relativi all'accesso a dati personali e sensibili

La tabella seguente descrive i requisiti relativi ad attività specifiche.

Attività	Requisito
L'app raccoglie o collega identificatori dei dispositivi persistenti (ad esempio IMEI, IMSI, numero di serie della SIM e così via)	Gli identificatori dei dispositivi persistenti non possono essere collegati ad altri dati utente personali e sensibili o a identificatori dei dispositivi reimpostabili, se non per le seguenti finalità: • servizi di telefonia collegati a un'identità SIM (ad esempio chiamate Wi-Fi collegate all'account di un operatore); e • app di gestione di dispositivi aziendali, utilizzando la modalità proprietario del dispositivo. Questi utilizzi devono essere indicati in posizione ben visibile, come specificato nelle norme relative ai dati utente . Consulta questa risorsa per scoprire identificatori univoci alternativi. Leggi le norme relative agli annunci per avere ulteriori indicazioni relative all'ID pubblicità di Android.
L'app è rivolta a bambini e ragazzi	La tua app può includere solo SDK che dispongono dell'autocertificazione per l'utilizzo nei servizi rivolti ai minori. Consulta il Programma relativo all'SDK per gli annunci autocertificati per la famiglia per leggere il testo completo delle norme e i requisiti.

Esempi di violazioni causate dagli SDK

- Un'app che utilizza un SDK che collega l'ID Android e la posizione
- Un'app con un SDK che collega l'AAID agli identificatori del dispositivo persistenti per qualsiasi scopo pubblicitario o di analisi.
- Un'app che utilizza un SDK che collega l'AAID e l'indirizzo email per scopi di analisi.

Sezione Sicurezza dei dati

Tutti gli sviluppatori sono tenuti a compilare in modo chiaro e preciso una sezione Sicurezza dei dati per ogni app, fornendo spiegazioni dettagliate in merito alla raccolta, all'utilizzo e alla condivisione dei dati utente. Sono inclusi i dati raccolti e gestiti tramite librerie o SDK di terze parti usati nelle loro app. Lo sviluppatore è responsabile dell'esattezza dell'etichetta e di mantenere aggiornate queste informazioni. Ove pertinente, la sezione deve essere conforme alle informative presenti nelle norme sulla privacy dell'app.

Leggi questo articolo del Centro assistenza per ulteriori informazioni sulla compilazione della sezione Sicurezza dei dati.

Consulta le norme relative ai dati utente complete.

Norme relative ad autorizzazioni e API che accedono a informazioni sensibili

Le richieste di autorizzazioni e di API che accedono a informazioni sensibili dovrebbero essere sensate per gli utenti. Puoi richiedere solo le autorizzazioni e le API che accedono a informazioni sensibili necessarie per implementare funzionalità o servizi esistenti della tua app che vengono promossi nella scheda di Google Play. Non puoi utilizzare le autorizzazioni o le API che accedono a informazioni sensibili che consentono l'accesso ai dati dell'utente o del dispositivo per funzionalità o scopi non dichiarati, non implementati o non consentiti. I dati personali o sensibili accessibili tramite le autorizzazioni o le API che hanno accesso a informazioni sensibili non possono mai essere venduti né condivisi con lo scopo di facilitare la vendita.

Consulta le Norme relative ad autorizzazioni e API che accedono a informazioni sensibili.

Esempi di violazioni causate dagli SDK

- La tua app include un SDK che richiede la posizione in background per uno scopo non consentito o non dichiarato.
- La tua app include un SDK che trasmette l'IMEI derivato dall'autorizzazione read_phone_state di Android senza il consenso dell'utente.

Norme relative al malware

Le nostre norme relative al malware sono semplici: l'ecosistema Android, incluso il Google Play Store, e i dispositivi degli utenti dovrebbero essere privi di comportamenti dannosi, come i malware. Sulla base di questo principio fondamentale, ci impegniamo per offrire un ecosistema Android sicuro per i nostri utenti e i loro dispositivi.

App o codice di terze parti (ad esempio, un SDK) con linguaggi interpretati (JavaScript, Python, Lua e così via) caricati in fase di runtime (ad esempio, non inclusi nell'app) non devono consentire potenziali violazioni delle norme di Google Play.

I requisiti di queste norme si applicano anche a qualsiasi codice di terze parti (ad esempio, un SDK) incluso nella tua app.

Consulta le norme relative al malware complete.

Esempi di violazioni causate dagli SDK

- Un'app che include librerie SDK di fornitori che distribuiscono software dannoso.
- Un'app che viola il modello di autorizzazioni Android o sottrae le credenziali (ad esempio, i token OAuth) da altre app.

- App che utilizzano funzionalità in modo illecito per evitare disinstallazione o arresto.
- Un'app che disattiva SELinux.
- Un'app che include un SDK che viola il modello di autorizzazioni Android ottenendo privilegi elevati tramite l'accesso ai dati sul dispositivo per uno scopo non dichiarato.
- Un'app che include un SDK con codice che induce con l'inganno gli utenti ad abbonarsi a contenuti o ad acquistarli tramite la fatturazione con l'operatore telefonico.

Le app di escalation dei privilegi che eseguono il rooting dei dispositivi senza l'autorizzazione dell'utente sono classificate come app di rooting.

Spyware

Lo spyware è un'applicazione, un codice o un comportamento dannoso che raccoglie, esfiltra o condivide dati di utenti o dispositivi non correlati alla funzionalità conforme alle norme.

Sono ritenuti spyware anche codici o comportamenti dannosi che possono essere considerati come spionaggio a danno dell'utente o che esfiltrano dati senza adeguato preavviso o consenso.

Consulta le norme relative agli spyware complete.

Ad esempio, le violazioni da parte di spyware causate dagli SDK includono, a titolo esemplificativo:

- Un'app che utilizza un SDK che trasmette i dati di registrazioni audio o delle chiamate non correlati alla funzionalità dell'app conforme alle norme.
- Un'app con codice dannoso di terze parti (ad esempio un SDK) che trasmette dati dal dispositivo in una modalità inaspettata per l'utente e/o senza un adeguato preavviso o consenso da parte dell'utente.

Norme relative al software mobile indesiderato

Comportamento trasparente e informative chiare

Tutto il codice deve rispettare le promesse fatte all'utente. Le app devono fornire tutte le funzionalità comunicate. Le app non devono confondere gli utenti.

Esempi di violazioni:

- Frode pubblicitaria
- Ingegneria sociale

Proteggere i dati utente

È necessario essere chiari e trasparenti in merito ad accesso, utilizzo, raccolta e condivisione di dati utente personali e sensibili. L'utilizzo dei dati utente deve rispettare tutte le Norme sui dati utente pertinenti, ove applicabili, e adottare tutte le misure necessarie per proteggere questi dati.

Esempi di violazioni:

- Raccolta dei dati (vedi Spyware)
- Utilizzo illecito di autorizzazioni limitate

Consulta le Norme relative al software mobile indesiderato

Norme sull'utilizzo illecito di dispositivi e reti

Sono vietate le app che interrompono, danneggiano, interferiscono con il funzionamento o accedono in modo non autorizzato al dispositivo dell'utente, altri dispositivi o computer, server, reti, API (interfacce di programmazione di un'applicazione) o servizi inclusi, a titolo esemplificativo, altre app sul dispositivo, servizi di Google o la rete di un operatore autorizzato.

App o codice di terze parti (ad esempio, un SDK) con linguaggi interpretati (JavaScript, Python, Lua e così via) caricati in fase di runtime (ad esempio, non inclusi nell'app) non devono consentire potenziali violazioni delle norme di Google Play.

È vietato il codice che introduce o sfrutta vulnerabilità di sicurezza. Consulta il Programma App Security Improvement per scoprire i problemi di sicurezza più recenti segnalati agli sviluppatori.

Consulta le norme sull'utilizzo illecito di dispositivi e reti.

Esempi di violazioni causate dagli SDK

- Le app che agevolano servizi di proxy verso terze parti sono consentite solo laddove questo sia lo scopo principale dell'app rivolto all'utente.
- La tua app include un SDK che scarica codice eseguibile, come file dex o codice nativo, da un'origine diversa da Google Play.
- La tua app include un SDK contenente un componente WebView con interfaccia JavaScript aggiunta che carica contenuti web non attendibili (ad esempio, URL http://) oppure URL non verificati derivanti da fonti non attendibili (ad esempio, URL derivanti da intent non attendibili).
- La tua app include un SDK che contiene codice utilizzato per l'aggiornamento del proprio APK.
- La tua app include un SDK che espone gli utenti a una vulnerabilità di sicurezza scaricando i file su una connessione non sicura.
- La tua app utilizza un SDK che contiene codice per scaricare o installare applicazioni da origini sconosciute al di fuori di Google Play.
- La tua app include un SDK che utilizza servizi in primo piano senza un caso d'uso adeguato.
- La tua app include un SDK che utilizza servizi in primo piano per un motivo conforme alle norme, ma non è dichiarato nel file manifest dell'app.

Norme relative ai comportamenti ingannevoli

Sono vietate le app che cercano di ingannare gli utenti o di favorire comportamenti disonesti incluse, a titolo esemplificativo ma non esaustivo, tutte le app il cui funzionamento sia determinato essere impossibile. Le app devono contenere comunicazioni, descrizioni e immagini/video precisi relativi alla loro funzionalità in ogni parte dei metadati. Non devono cercare di imitare funzionalità o avvisi del sistema operativo o di altre app. Eventuali modifiche alle impostazioni del dispositivo non devono essere apportate all'insaputa e senza il consenso dell'utente, che deve poterle annullare.

Consulta le norme relative ai comportamenti ingannevoli complete.

Trasparenza del comportamento

La funzionalità della tua app deve essere ragionevolmente chiara agli utenti; non includere funzionalità nascoste, inattive o non provviste di documentazione nella tua app. Non sono consentite tecniche per evitare i controlli delle app. Alle app potrebbe essere richiesto di fornire ulteriori dettagli per garantire la sicurezza degli utenti, l'integrità del sistema e la conformità alle norme.

Esempio di violazione causata dall'SDK

- La tua app include un SDK che utilizza tecniche per evitare i controlli delle app.

Quali norme per gli sviluppatori di Google Play sono comunemente associate alle violazioni causate dagli SDK?

Per aiutarti a garantire che qualsiasi codice di terze parti utilizzato dalla tua app sia conforme alle Norme del programma per gli sviluppatori di Google Play, consulta le seguenti norme nella loro interezza:

- Norme relative ai dati utente
- Autorizzazioni e API che accedono a informazioni sensibili
- Norme relative all'utilizzo illecito di dispositivi e reti

- Malware
- Software mobile indesiderato
- Programma relativo all'SDK per gli annunci autocertificati per la famiglia
- Norme relative agli annunci
- Comportamento ingannevole
- Norme del programma per gli sviluppatori di Google Play

Sebbene queste norme siano più comunemente oggetto di discussione, è importante ricordare che un codice SDK errato potrebbe far sì che l'app violi un'altra norma non menzionata sopra. Ricorda di rivedere tutte le norme nella loro interezza e di tenerti sempre al passo con i relativi aggiornamenti, in quanto è tua responsabilità, come sviluppatore di app, assicurarti che gli SDK gestiscano i dati delle tue app in modo conforme alle norme.

Per saperne di più, visita il nostro Centro assistenza.

Malware

Le nostre norme relative al malware sono semplici: l'ecosistema Android, incluso il Google Play Store, e i dispositivi degli utenti dovrebbero essere privi di comportamenti dannosi, come i malware. Sulla base di questo principio fondamentale, ci impegniamo per offrire un ecosistema Android sicuro per i nostri utenti e i loro dispositivi.

App o codice di terze parti (ad esempio, un SDK) con linguaggi interpretati (JavaScript, Python, Lua e così via) caricati in fase di runtime (ad esempio, non inclusi nell'app) non devono consentire potenziali violazioni delle norme di Google Play.

I requisiti di queste norme si applicano anche a qualsiasi codice di terze parti (ad esempio, un SDK) incluso nella tua app.

Sebbene siano diversi per tipologia e capacità, i malware in genere hanno uno dei seguenti obiettivi:

- Compromettere l'integrità del dispositivo dell'utente.
- Assumere il controllo del dispositivo dell'utente.
- Attivare operazioni controllate a distanza affinché un utente malintenzionato possa accedere, utilizzare o altrimenti sfruttare un dispositivo infetto.
- Trasmettere dati personali o credenziali dal dispositivo senza adeguata comunicazione e senza il consenso dell'utente.
- Diffondere spam o comandi dal dispositivo infetto per colpire altri dispositivi o reti.
- Defraudare l'utente.

La modifica di un framework, un programma binario o un'app può essere potenzialmente pericolosa e pertanto generare comportamenti dannosi, anche in modo non intenzionale. Ciò avviene perché le modifiche di framework, programmi binari o app possono dar luogo a funzionamenti diversi in base a una serie di variabili. Pertanto, ciò che è dannoso per un dispositivo Android potrebbe non porre alcun rischio per un altro. Ad esempio, un dispositivo con la versione più recente di Android non è interessato da app dannose che utilizzano API deprecate per eseguire comportamenti dannosi, ma un dispositivo con una delle prime versioni di Android potrebbe essere a rischio. Modifiche di app, programmi binari o framework vengono segnalate come malware o app potenzialmente dannose se rappresentano un rischio evidente per alcuni o per tutti i dispositivi Android e gli utenti.

Le categorie di malware indicate di seguito riflettono la nostra profonda convinzione secondo cui gli utenti dovrebbero capire come il loro dispositivo viene sfruttato e contribuire alla sicurezza di un ecosistema che garantisca innovazioni valide e un'esperienza utente affidabile.

Visita Google Play Protect per maggiori informazioni.

Backdoor

Codice che consente l'esecuzione su un dispositivo di operazioni controllate a distanza, indesiderate e potenzialmente dannose.

Queste operazioni potrebbero includere un comportamento che, se eseguito automaticamente, determinerebbe l'inclusione della modifica a framework, programmi binari o app in una delle altre categorie di malware. In generale, con il termine backdoor si descrive la modalità con cui un'operazione potenzialmente dannosa può verificarsi su un dispositivo, pertanto il termine non corrisponde esattamente a categorie quali frode di fatturazione o spyware commerciale. Conseguentemente, un sottoinsieme di backdoor, in determinate circostanze, viene considerato da Google Play Protect come una vulnerabilità.

Frode di fatturazione

Codice che effettua addebiti automatici agli utenti in modo intenzionalmente ingannevole.

La frode di fatturazione su dispositivi mobili può essere: frode tariffaria, SMS fraudolento o chiamata fraudolenta.

SMS fraudolento
Codice che effettua addebiti agli utenti per l'invio di SMS a pagamento senza il loro consenso o che cerca di camuffare le sue attività SMS nascondendo gli accordi di divulgazione o gli SMS dell'operatore di telefonia mobile che informano gli utenti degli addebiti o che confermano gli abbonamenti.

Esiste del codice che, anche se tecnicamente comunica il comportamento di invio degli SMS, introduce un comportamento aggiuntivo che consente l'SMS fraudolento. Ecco alcuni esempi: nascondere parti di un accordo di divulgazione agli utenti o renderle illeggibili ed eliminare condizionalmente gli SMS dell'operatore di telefonia mobile che informano gli utenti degli addebiti o confermano un abbonamento.

Chiamata fraudolenta
Codice che effettua addebiti agli utenti chiamando numeri a pagamento senza il consenso degli utenti.

Frode tariffaria
Codice che induce con l'inganno gli utenti ad abbonarsi a contenuti o ad acquistarli tramite il loro conto telefonico.

La frode tariffaria include qualsiasi tipo di fatturazione ad eccezione di SMS e chiamate verso numerazioni a sovrapprezzo. Ecco alcuni esempi: fatturazione diretta con l'operatore, punto di accesso wireless (WAP) e trasferimento di credito tra dispositivi mobili. La frode WAP è uno dei tipi di frode tariffaria più usati. Chi attua questo tipo di frode potrebbe indurre con l'inganno gli utenti a fare clic su un pulsante in un componente WebView trasparente caricato in modo invisibile. Questa azione avvia un abbonamento ricorrente e l'email o l'SMS di conferma vengono spesso compromessi per evitare che gli utenti si accorgano della transazione finanziaria.

Stalkerware

Codice che raccoglie dati utente personali o sensibili da un dispositivo e li trasmette a una terza parte (un'azienda o un privato) a fini di monitoraggio.

Le app devono contenere un'informativa ben visibile adeguata e ottenere il consenso come richiesto dalle norme relative ai dati utente .

Linee guida per le applicazioni di monitoraggio

Purché soddisfino completamente i requisiti descritti di seguito, le app progettate e commercializzate esclusivamente per il monitoraggio di un'altra persona, ad esempio per il monitoraggio dei figli da parte dei genitori o per il monitoraggio di singoli dipendenti da parte dei responsabili aziendali, sono le uniche app di monitoraggio accettabili. Queste app non possono essere utilizzate per monitorare altre persone (ad esempio il coniuge) anche se con il loro consenso e la loro autorizzazione, a prescindere

dalla visualizzazione di una notifica persistente. Per poter essere classificate in modo appropriato come app di monitoraggio, queste app devono usare il flag dei metadati IsMonitoringTool nel proprio file manifest.

Le app di monitoraggio devono soddisfare i seguenti requisiti:

- Le app non devono essere presentate come soluzioni per spionaggio o sorveglianza segreta.
- Le app non devono nascondere o mascherare il comportamento di monitoraggio oppure tentare di ingannare gli utenti in merito a questa funzionalità.
- Le app devono presentare agli utenti una notifica persistente per tutto il tempo in cui sono in esecuzione e un'icona univoca che le identifichi chiaramente.
- Le app devono comunicare la funzionalità di monitoraggio o tracciamento nella descrizione del Google Play Store.
- Le app e le relative schede su Google Play non devono consentire in alcun modo di attivare o accedere a funzionalità che violano i presenti termini, ad esempio link che rimandano a un APK non conforme non ospitato su Google Play.
- Le app devono rispettare tutte le leggi applicabili. È tua esclusiva responsabilità determinare la legalità della tua app nelle località di destinazione.

Per ulteriori informazioni, leggi l'articolo del Centro assistenza Uso del flag isMonitoringTool .

Denial of service (DoS)

Codice che, a insaputa dell'utente, esegue un attacco denial of service (DoS) o fa parte di un attacco DoS distribuito contro altri sistemi e risorse.

Ad esempio, l'attacco potrebbe consistere nell'invio di un volume elevato di richieste HTTP per sovraccaricare server remoti.

Downloader ostili

Codice che non è potenzialmente dannoso di per sé, ma che scarica altre app potenzialmente dannose.

Il codice potrebbe essere un downloader ostile se:

- Esiste motivo di ritenere che sia stato creato per diffondere app potenzialmente dannose e che abbia scaricato tali app o che contenga codice che potrebbe scaricare e installare app; oppure
- Almeno il 5% delle app scaricate dal codice è formato da app potenzialmente dannose con una soglia minima di 500 download di app osservate (25 download di app potenzialmente dannose osservate).

I principali browser e app per la condivisione di file non sono considerati downloader ostili se:

- Non favoriscono download senza interazione dell'utente; e
- Tutti i download di app potenzialmente dannose vengono attivati da utenti consenzienti.

Minaccia non Android

Codice contenente minacce non Android.

Queste app non possono danneggiare l'utente o il dispositivo Android, ma contengono componenti potenzialmente dannosi per altre piattaforme.

Phishing

Codice che finge di provenire da una fonte affidabile, richiede le credenziali per l'autenticazione o i dati di fatturazione dell'utente e invia tali dati a una terza parte. Questa categoria, inoltre, si applica al codice che intercetta la trasmissione delle credenziali dell'utente in transito.

Tra gli obiettivi di phishing comuni, credenziali bancarie, numeri di carte di credito e credenziali di account online per social network e giochi.

Abuso di privilegio elevato

Codice che compromette l'integrità del sistema violando la sandbox dell'app, ottenendo privilegi elevati o modificando o disattivando l'accesso alle principali funzioni correlate alla sicurezza.

Tra gli esempi possibili:

- Un'app che viola il modello di autorizzazioni Android o sottrae le credenziali (ad esempio, i token OAuth) da altre app.
- App che abusano di funzionalità per evitare di essere disinstallate o arrestate.
- Un'app che disattiva SELinux.

Le app di escalation dei privilegi che eseguono il rooting dei dispositivi senza l'autorizzazione dell'utente sono classificate come app di rooting.

Ransomware

Codice che assume il controllo parziale o totale di un dispositivo o dei dati su un dispositivo ed esige dall'utente un pagamento o un'azione per rilasciare il controllo.

Alcuni tipi di ransomware criptano i dati sul dispositivo ed esigono un pagamento per decriptare i dati e/o sfruttano le funzionalità di amministratore del dispositivo in modo che il ransomware non possa essere rimosso da un utente medio. Tra gli esempi possibili:

- Impedire all'utente di accedere al dispositivo ed esigere denaro in cambio del ripristino del controllo da parte dell'utente.
- Criptare i dati sul dispositivo ed esigere un pagamento, verosimilmente in cambio della decriptazione dei dati.
- Sfruttare le funzionalità di Gestione norme del dispositivo e bloccare la rimozione da parte dell'utente.

Eventuale codice distribuito con il dispositivo la cui finalità primaria sia la gestione di un dispositivo sovvenzionato può essere escluso dalla categoria del ransomware, a condizione che soddisfi i requisiti per la gestione e il blocco sicuri, nonché i requisiti di comunicazione e consenso adeguati da parte dell'utente.

Rooting

Codice che esegue il rooting del dispositivo.

C'è una differenza tra codice di rooting non dannoso e dannoso. Ad esempio, le app di rooting non dannoso consentono agli utenti di sapere in anticipo che stanno per eseguire il rooting del dispositivo e non eseguono altre azioni potenzialmente dannose che riguardano altre categorie di app potenzialmente dannose.

Le app di rooting dannoso non comunicano agli utenti che stanno per eseguire il rooting del dispositivo e non li informano anticipatamente del rooting; eseguono inoltre altre azioni che riguardano altre categorie di app potenzialmente dannose.

Spam

Codice che invia messaggi non richiesti ai contatti dell'utente o che utilizza il dispositivo per l'inoltro di spam via email.

Spyware

Lo spyware è un'applicazione, un codice o un comportamento dannoso che raccoglie, esfiltra o condivide dati di utenti o dispositivi non correlati alla funzionalità conforme alle norme.

Sono ritenuti spyware anche codici o comportamenti dannosi che possono essere considerati come spionaggio a danno dell'utente o che esfiltrano dati senza adeguato preavviso o consenso.

Ad esempio, le violazioni degli spyware includono, a titolo esemplificativo:

- Registrazione di audio o di chiamate ricevute sul telefono.
- Furto di dati dell'app.
- Un'app con codice dannoso di terze parti (ad esempio un SDK) che trasmette dati dal dispositivo in una modalità inaspettata per l'utente e/o senza un adeguato preavviso o consenso da parte dell'utente.

Tutte le app devono inoltre rispettare tutte le Norme del programma per gli sviluppatori di Google Play, comprese le norme relative ai dati degli utenti e dei dispositivi, ad esempio quelle relative a software mobile indesiderato, dati utente, autorizzazioni e API che accedono a informazioni sensibili e requisiti relativi all'SDK.

Trojan

Codice apparentemente innocuo, ad esempio un gioco che dichiara di essere esclusivamente tale, ma che esegue azioni indesiderate nei confronti dell'utente.

In genere questa classificazione è utilizzata insieme ad altre categorie di app potenzialmente dannose. Un trojan ha un componente innocuo e un componente dannoso nascosto. Ad esempio, un gioco che invia messaggi SMS premium dal dispositivo dell'utente in background e senza che l'utente ne sia a conoscenza.

Una nota sulle app non comuni

Le app nuove e meno diffuse possono essere classificate come non comuni se Google Play Protect non dispone di informazioni sufficienti per autorizzarle come app sicure. Ciò non significa che l'app è necessariamente dannosa, ma in assenza di un'ulteriore revisione non può nemmeno essere autorizzata come app sicura.

Una nota sulla categoria Backdoor

La classificazione della categoria di malware backdoor si basa sulla modalità con cui il codice agisce. Una condizione necessaria affinché un codice venga classificato come backdoor è che consenta un comportamento che, se eseguito automaticamente, determinerebbe l'inclusione del codice in una delle altre categorie di malware. Ad esempio, se un'app consente il caricamento di codice dinamico e il codice caricato dinamicamente estrae SMS, l'app verrà classificata come malware backdoor.

Tuttavia, se un'app consente l'esecuzione arbitraria di codice e non abbiamo ragione di credere che tale esecuzione sia stata aggiunta al fine di dar luogo a un comportamento malevolo, l'app verrà considerata come contenente una vulnerabilità, anziché essere definita malware backdoor, e allo sviluppatore verrà chiesto di creare una patch per l'app medesima.

Maskware

Un'applicazione che utilizza una varietà di tecniche di evasione per offrire all'utente funzionalità dell'applicazione diverse o false. Queste app si mascherano da applicazioni o giochi legittimi per apparire innocue agli store e utilizzano tecniche quali l'offuscamento, il caricamento di codice dinamico o il cloaking per rivelare i contenuti dannosi.

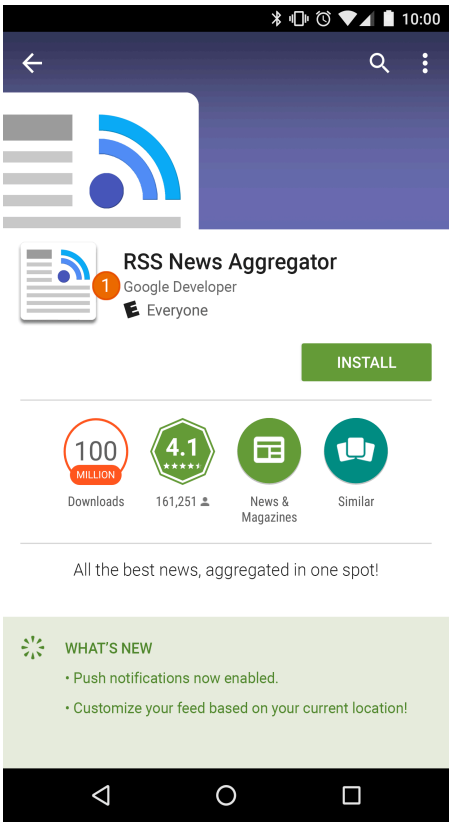
Il maskware è simile ad altre categorie di app potenzialmente dannose, in particolare ai Trojan; la differenza principale sono le tecniche utilizzate per offuscare l'attività dannosa.

Furto d'identità

Sono vietate le app che ingannano gli utenti assumendo l'identità di altri soggetti (ad esempio, altri sviluppatori, aziende, persone giuridiche) o di un'altra app. Evita di lasciar falsamente intendere che l'app sia collegata o autorizzata da qualcuno. Fai attenzione a non utilizzare icone dell'app, descrizioni, titoli o elementi in-app che potrebbero fuorviare gli utenti in merito alla relazione della tua app con un altro soggetto o con un'altra app.

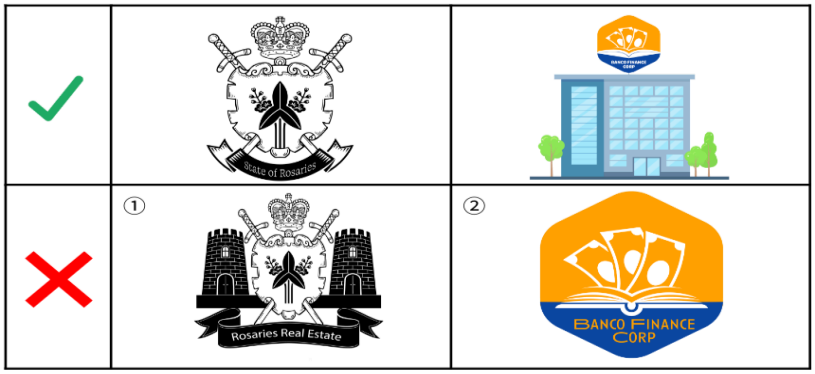
Di seguito sono riportati alcuni esempi di violazioni frequenti:

- Sviluppatori che lasciano falsamente intendere l'esistenza di una relazione con un'altra società, persona giuridica, organizzazione o con un altro sviluppatore.



① Il nome dello sviluppatore indicato per l'app suggerisce una relazione ufficiale con Google, che in realtà non esiste.

- App i cui titoli e icone lasciano falsamente intendere l'esistenza di una relazione con un'altra società, persona giuridica, organizzazione o con un altro sviluppatore.



① L'app usa un emblema nazionale e induce gli utenti a credere di essere affiliata con il governo.
② L'app copia il logo di una persona giuridica aziendale per suggerire in modo ingannevole di essere l'app ufficiale dell'azienda.

- Titoli e icone di app talmente simili a quelli di prodotti o servizi esistenti da poter trarre in inganno gli utenti.

① L'app usa il logo del sito web di una nota criptovaluta nella propria icona per suggerire di essere il sito web ufficiale.
② L'app copia il personaggio e il titolo di un noto programma TV nella propria icona inducendo gli utenti a credere di essere affiliata al programma TV.

- App che dichiarano falsamente di essere le app ufficiali di un'entità riconosciuta. Titoli quali "App ufficiale di Justin Bieber" sono vietati senza le autorizzazioni o i diritti necessari.
- App che violano le linee guida per il brand Android .

Software indesiderato per dispositivi mobili

Noi di Google riteniamo che se ci concentriamo sull'utente, tutto il resto viene da sé. Nei nostri Principi sul software e nelle Norme relative al software indesiderato, forniamo consigli generali per software che offrano un'ottima esperienza utente. Questa norma si basa sulle Norme relative al software indesiderato di Google definendo i principi per l'ecosistema Android e il Google Play Store. Il software che vìola tali princìpi può influire nativamente sull'esperienza degli utenti: per questo adottiamo misure per tutelarli.

Come indicato nelle Norme relative al software indesiderato, abbiamo riscontrato che la maggior parte dei software indesiderati presenta una o più delle stesse caratteristiche di base:

- È ingannevole in quanto promette un valore aggiunto che non offre.
- Cerca di indurre con l'inganno gli utenti a installarlo o si cela all'interno di un altro programma installato dall'utente.
- Non illustra all'utente tutte le proprie funzioni principali e distintive.
- Altera il sistema dell'utente in modi inaspettati.
- Raccoglie o trasmette informazioni private a insaputa degli utenti.
- Raccoglie o trasmette informazioni private senza una gestione sicura (ad esempio, trasmissione tramite HTTPS)
- È integrato in un altro software senza che la sua presenza venga esplicitata.

Sui dispositivi mobili, il software è codice sotto forma di app, programma binario, modifica del framework e così via. Per bloccare software dannosi per l'ecosistema informatico o che influenzano negativamente l'esperienza utente, prendiamo provvedimenti sul codice che vìola questi principi.

Di seguito, estendiamo l'applicabilità delle Norme relative al software indesiderato anche al software per dispositivi mobili. Come per quelle norme, continueremo a perfezionare queste Norme relative al software indesiderato per dispositivi mobili in modo da affrontare nuovi tipi di violazioni.

Comportamento trasparente e informative chiare

Tutto il codice deve rispettare le promesse fatte all'utente. Le app devono fornire tutte le funzionalità comunicate. Le app non devono confondere gli utenti.

- Le app devono indicare chiaramente la propria funzionalità e i propri obiettivi.
- Lo sviluppatore deve spiegare in modo chiaro ed esplicito le modifiche che verranno apportate dall'app al sistema e consentire agli utenti di esaminare e approvare tutte le modifiche e le opzioni di installazione significative.
- Il software non deve rappresentare in modo ingannevole lo stato del dispositivo dell'utente, ad esempio dichiarando che il sistema è in uno stato di sicurezza critico o infettato da virus.
- Lo sviluppatore deve evitare di utilizzare attività non valide concepite per aumentare il traffico dagli annunci pubblicitari e/o le conversioni.
- Sono vietate le app che ingannano gli utenti assumendo l'identità di un altro soggetto (ad esempio, altri sviluppatori, aziende, persone giuridiche) o di un'altra app. Lo sviluppatore deve evitare di lasciare falsamente intendere che l'app sia collegata a un altro soggetto o da questo autorizzata.

Esempi di violazioni:

- Frode pubblicitaria
- Ingegneria sociale

Proteggere i dati e la privacy degli utenti

È necessario essere chiari e trasparenti in merito ad accesso, utilizzo, raccolta e condivisione di dati utente personali e sensibili. L'utilizzo dei dati utente deve ottemperare a tutte le norme relative ai dati utente pertinenti, ove applicabili, e adottare tutte le misure necessarie per proteggere questi dati.

- Devi fornire agli utenti l'opportunità di prestare il consenso alla raccolta dei loro dati prima di iniziare a raccoglierli e inviarli dal dispositivo, ciò include i dati relativi ad account di terze parti, email, numero di telefono, app installate, file, posizione e qualsiasi altro dato personale e sensibile del quale l'utente non si aspetti la raccolta.
- I dati utente personali e sensibili che vengono raccolti devono essere gestiti in modo sicuro, inclusa la trasmissione mediante metodi moderni di crittografia (ad esempio, tramite HTTPS).
- Il software, incluse le app mobile, deve trasmettere ai server dati utente personali e sensibili solo nella misura in cui siano correlati alla funzionalità dell'app.
- Non ingannare gli utenti inducendoli a disattivare le protezioni di sicurezza del dispositivo come Google Play Protect e non richiedere loro di farlo. Ad esempio, non devi offrire agli utenti funzionalità aggiuntive dell'app o premi in cambio della disattivazione di Google Play Protect.

Esempi di violazioni:

- Raccolta dei dati (vedi Spyware)
- Abuso di autorizzazioni limitate

Esempi di norme relative ai dati utente:

- Norme relative ai dati utente di Google Play
- Norme relative ai dati utente dei requisiti GMS
- Norme relative ai dati utente del servizio API di Google

Non compromettere l'esperienza su dispositivi mobili

L'esperienza utente deve essere lineare, facile da capire e basata su scelte chiare effettuate dall'utente. Deve presentare all'utente una proposta di valore chiara e non interrompere l'esperienza utente pubblicizzata o desiderata.

- Lo sviluppatore deve evitare annunci che vengono mostrati agli utenti in modi imprevisti, ad esempio compromettendo l'usabilità delle funzionalità del dispositivo o interferendo con la stessa, o visualizzando tali annunci al di fuori dell'app senza che sia possibile chiuderli facilmente e senza consenso e attribuzione adeguati.
- Le app non devono interferire con altre app o con l'usabilità del dispositivo.
- La possibilità di procedere alla disinstallazione, se applicabile, deve essere chiara.
- Il software per dispositivi mobili non deve imitare le richieste del sistema operativo del dispositivo o di altre app. Lo sviluppatore non deve eliminare gli avvisi all'utente da altre app o dal sistema operativo, in particolare quelli che lo informano delle modifiche al sistema operativo.

Esempi di violazioni:

- Annunci improvvisi
- Utilizzo non autorizzato o imitazione di funzionalità di sistema

---

Downloader ostili

Codice che non è software indesiderato di per sé, ma che scarica altro software indesiderato per dispositivi mobili.

Il codice potrebbe essere un downloader ostile se:

- Esiste motivo di ritenere che sia stato creato per diffondere software indesiderato per dispositivi mobili e che abbia scaricato tale software o che contenga codice che potrebbe scaricare e installare app; oppure
- Almeno il 5% delle app scaricate dal codice è costituito da software indesiderato per dispositivi mobili con una soglia minima di 500 download di app osservati (25 download di software indesiderato per dispositivi mobili osservati).

I principali browser e app per la condivisione di file non sono considerati downloader ostili se:

- Non favoriscono download senza interazione dell'utente; e
- Tutti i download di software vengono avviati da utenti consenzienti.

Frode pubblicitaria

La frode pubblicitaria è severamente vietata. Le interazioni con gli annunci generate allo scopo di indurre una rete pubblicitaria a ritenere che il traffico provenga da un autentico interesse dell'utente è considerata frode pubblicitaria, una forma di traffico non valido. Le frodi pubblicitarie possono essere il sottoprodotto dell'implementazione di annunci in modi non consentiti da parte degli sviluppatori, ad esempio visualizzazione di annunci nascosti, clic automatico sugli annunci, alterazione o modifica di informazioni e altre modalità di utilizzo di azioni non umane (spider, bot e così via) o di attività umane concepite per generare traffico dagli annunci pubblicitari non valido. Il traffico non valido e le frodi pubblicitarie sono dannosi per inserzionisti, sviluppatori e utenti e comportano una perdita di fiducia a lungo termine nell'ecosistema degli annunci per dispositivi mobili.

Di seguito sono riportati alcuni esempi di violazioni frequenti:

- App che mostra annunci non visibili all'utente.
- App che genera automaticamente clic sugli annunci senza l'intenzione dell'utente o che genera traffico di rete equivalente per assegnare in modo fraudolento i crediti relativi ai clic.
- App che invia clic di attribuzione di installazione non veritieri per ricevere pagamenti per installazioni che non provengono dalla rete del mittente.

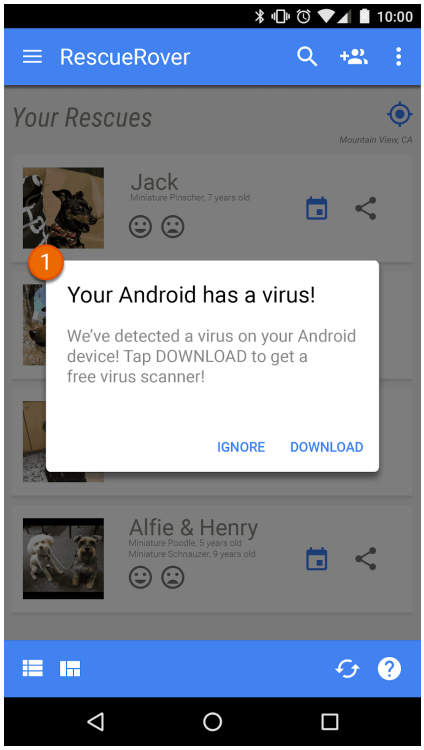
- App che mostra annunci quando l'utente non si trova nella sua interfaccia.
- False dichiarazioni dell'inventario pubblicitario da parte di un'app, ad esempio un'app che comunica alle reti pubblicitarie che è in esecuzione su un dispositivo iOS quando in realtà è installata su Android o un'app che rappresenta in modo ingannevole il nome del pacchetto che viene monetizzato.

Utilizzo non autorizzato o imitazione di funzionalità di sistema

Non sono consentiti annunci o app che imitano o interferiscono con le funzionalità di sistema, ad esempio notifiche o avvisi. È possibile utilizzare le notifiche a livello di sistema soltanto per funzioni integranti di un'app, ad esempio l'app di una compagnia aerea che avvisa gli utenti di promozioni speciali o un gioco che avvisa gli utenti di promozioni in-game.

Di seguito sono riportati alcuni esempi di violazioni frequenti:

- App o annunci che vengono pubblicati tramite una notifica o un avviso di sistema:



① La notifica di sistema mostrata in questa app viene utilizzata per pubblicare un annuncio.

Per altri esempi relativi agli annunci, leggi le Norme relative agli annunci.

Ingegneria sociale

Sono vietate le app che si spacciano per un'altra app con l'intento di indurre con l'inganno gli utenti a compiere azioni che tali utenti volevano compiere nell'app attendibile originale.

Monetizzazione e annunci

Google Play supporta una serie di strategie di monetizzazione a vantaggio di sviluppatori e utenti, inclusi prodotti in-app, distribuzione a pagamento, abbonamenti e modelli basati su annunci. Per poter

garantire la migliore esperienza possibile agli utenti, gli sviluppatori sono tenuti a rispettare le presenti norme.

Pagamenti

1. Gli sviluppatori che addebitano i download delle app da Google Play devono utilizzare il sistema di fatturazione di Google Play come metodo di pagamento di queste transazioni.
2. Le app distribuite su Google Play che richiedono o accettano pagamenti per l'accesso a servizi o funzionalità in-app, inclusi funzionalità dell'app e prodotti o contenuti digitali (collettivamente definiti "acquisti in-app"), devono utilizzare il sistema di fatturazione di Google Play per queste transazioni, a meno che non si applichi la Sezione 3, 8 o 9.

   Esempi di servizi o funzionalità di app che richiedono l'utilizzo del sistema di fatturazione di Google Play includono, a titolo esemplificativo, acquisti in-app di:

   - articoli (ad esempio valute virtuali, vite extra, tempo di gioco aggiuntivo, articoli aggiuntivi, personaggi e avatar);
   - servizi in abbonamento (ad esempio fitness, giochi, incontri, istruzione, musica, video, upgrade di servizi e altri servizi con contenuti in abbonamento);
   - funzionalità o contenuti di app (ad esempio versioni senza annunci delle app o nuove funzionalità non disponibili nelle versioni gratuite); e
   - software e servizi cloud (ad esempio servizi di archiviazione dati, software per la produttività aziendale e software di gestione finanziaria).

3. Il sistema di fatturazione di Google Play non deve essere utilizzato nei casi indicati di seguito.
   a. Il pagamento riguarda principalmente:
      - l'acquisto o il noleggio di beni fisici (ad esempio generi alimentari, abbigliamento, articoli per la casa, elettronica);
      - l'acquisto di servizi fisici (ad esempio servizi di trasporto, servizi di pulizia, biglietti aerei, abbonamenti in palestra, consegna di cibo, biglietti per eventi dal vivo); o
      - una rimessa relativa al rendiconto della carta di credito o a una bolletta per pubblici servizi (ad esempio servizi di TV via cavo e di telecomunicazioni);

   b. i pagamenti includono pagamenti peer-to-peer, aste online e donazioni esenti da imposte;
   c. il pagamento riguarda contenuti o servizi che promuovono giochi e scommesse online, come descritto nella sezione App di giochi e scommesse delle Norme relative a concorsi, giochi e scommesse con vincite in denaro;
   d. il pagamento riguarda qualsiasi categoria di prodotto ritenuta inaccettabile ai sensi delle Norme relative ai contenuti del Centro pagamenti di Google.

      Nota: in alcuni mercati offriamo Google Pay per le app che vendono beni e/o servizi fisici. Per ulteriori informazioni, visita la nostra pagina per sviluppatori Google Pay .

4. Fatta eccezione per le condizioni descritte nelle Sezioni 3, 8 e 9, le app non possono indirizzare gli utenti a un metodo di pagamento diverso dal sistema di fatturazione di Google Play. Questo divieto include, a titolo esemplificativo, il reindirizzamento degli utenti ad altri metodi di pagamento tramite:
   - La scheda di un'app in Google Play;
   - Promozioni in-app correlate a contenuti acquistabili;
   - WebView, pulsanti, link, messaggi, pubblicità o altri inviti all'azione in-app; e
   - I flussi dell'interfaccia utente in-app, inclusi i flussi di creazione dell'account o di registrazione, che indirizzano gli utenti da un'app a un metodo di pagamento diverso dal sistema di fatturazione di Google Play nell'ambito di questi flussi.

5. Le valute virtuali in-app devono essere utilizzate soltanto all'interno dell'app o del gioco per cui sono state acquistate.
6. Gli sviluppatori devono informare in modo chiaro e preciso gli utenti in merito ai termini e ai prezzi della loro app o di eventuali funzionalità o abbonamenti in-app in vendita. I prezzi in-app devono corrispondere ai prezzi visualizzati nell'interfaccia di fatturazione di Google Play mostrata agli utenti. Se la descrizione del prodotto su Google Play fa riferimento a funzionalità in-app a cui viene applicato un costo specifico o aggiuntivo, la scheda dell'app deve indicare in modo chiaro agli utenti che l'accesso a tali funzionalità è a pagamento.
7. Le app e i giochi che offrono meccanismi per ricevere articoli virtuali randomizzati da un acquisto inclusi, a titolo esemplificativo, "loot box", devono indicare chiaramente le probabilità di ricevere questi articoli prima e in prossimità dell'acquisto.
8. A meno che non si applichino le condizioni descritte nella Sezione 3, gli sviluppatori di app distribuite su Google Play che richiedono o accettano pagamenti degli utenti in questi paesi/queste regioni per l'accesso agli acquisti in-app possono offrire agli utenti un sistema di fatturazione alternativo all'interno dell'app, oltre al sistema di fatturazione di Google Play, per le transazioni in questione. A questo scopo, devono compilare correttamente il modulo di dichiarazione relativo alla fatturazione per ogni rispettivo programma, nonché accettare i termini aggiuntivi e i requisiti del programma inclusi.
9. Gli sviluppatori di app distribuite su Google Play potrebbero indirizzare gli utenti dello Spazio economico europeo (SEE) al di fuori dall'app, anche per promuovere offerte per funzionalità e servizi digitali in-app. Gli sviluppatori che indirizzano gli utenti del SEE all'esterno dell'app devono compilare correttamente il modulo di dichiarazione per il programma, nonché accettare i termini aggiuntivi e i requisiti del programma inclusi.

Nota: per visualizzare le tempistiche e le domande frequenti relative a questa norma, visita il nostro Centro assistenza.

Annunci

Per mantenere un'esperienza di qualità, prendiamo in considerazione i contenuti, il pubblico, l'esperienza utente e il comportamento del tuo annuncio, nonché la sicurezza e la privacy. Consideriamo gli annunci e le offerte associate come parte della tua app, pertanto devono essere anch'essi conformi alle norme di Google Play. Abbiamo anche requisiti aggiuntivi per gli annunci se monetizzi un'app rivolta a bambini e ragazzi su Google Play.

Puoi anche leggere ulteriori informazioni sulle nostre relative alla promozione di app e alle schede dello store in questa pagina, incluso il modo in cui affrontiamo le pratiche di promozione ingannevoli.

Contenuti dell'annuncio

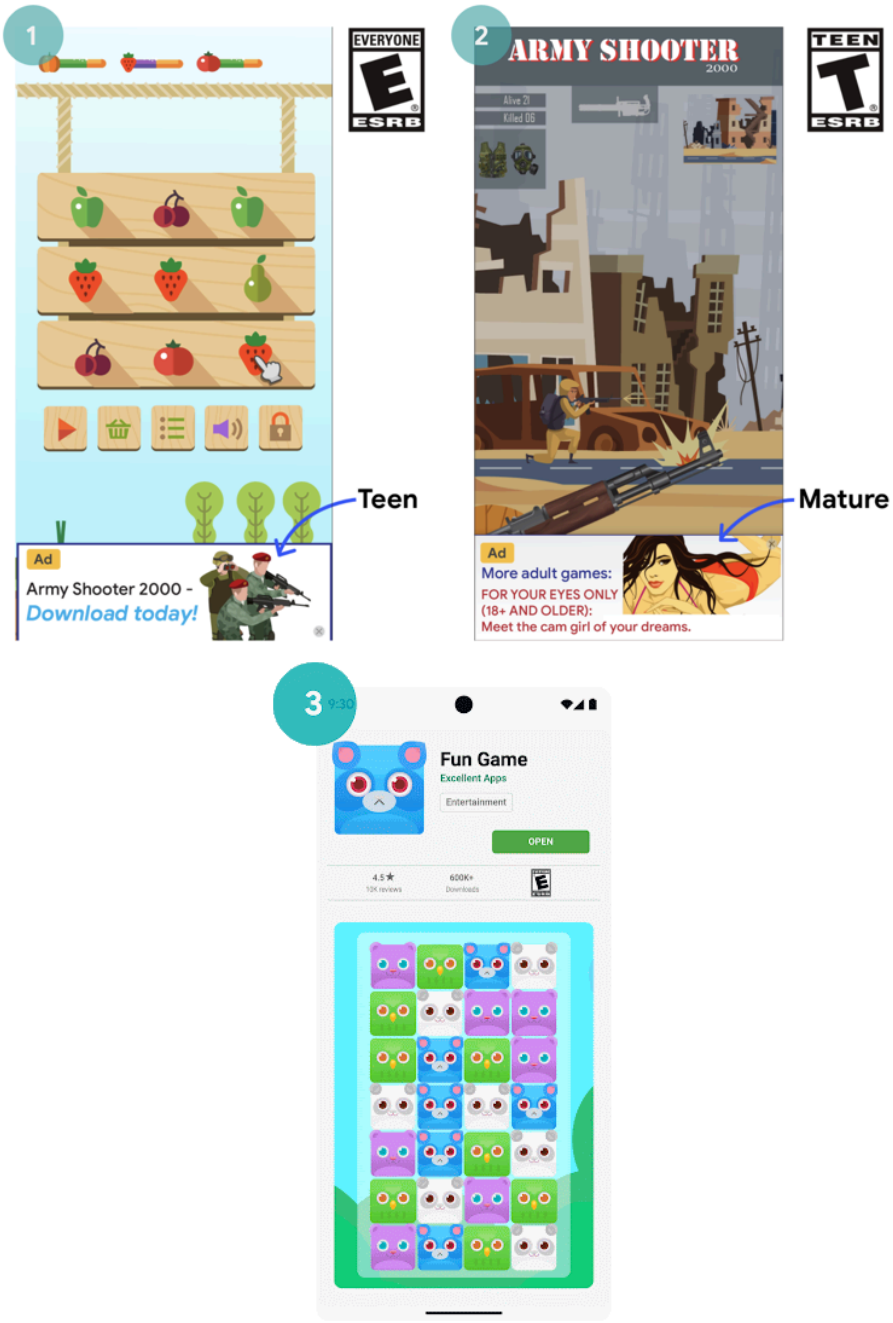
Gli annunci e le offerte associate fanno parte della tua app e devono rispettare le nostre norme relative ai contenuti con limitazioni. Se si tratta di un'app di giochi e scommesse, si applicano requisiti aggiuntivi.

Annunci inappropriati

Gli annunci e le offerte a essi associate (ad esempio, l'annuncio promuove il download di un'altra app) mostrati nella tua app devono essere appropriati per la relativa classificazione dei contenuti , anche se i contenuti stessi sono altrimenti conformi alle nostre norme.

Di seguito sono riportati alcuni esempi di violazioni frequenti:

- Gli annunci sono inappropriati per la classificazione dei contenuti dell'app



① Questo annuncio (Per adolescenti) non è appropriato per la classificazione dei contenuti dell'app (Per tutti)
② Questo annuncio (Per adulti) non è appropriato per la classificazione dei contenuti dell'app (Per adolescenti)
③ L'offerta dell'annuncio (che promuove il download di un'app Per adulti) non è appropriata per la classificazione dei contenuti dell'app di gioco in cui viene mostrata (Per tutti)

Requisiti degli annunci per le famiglie

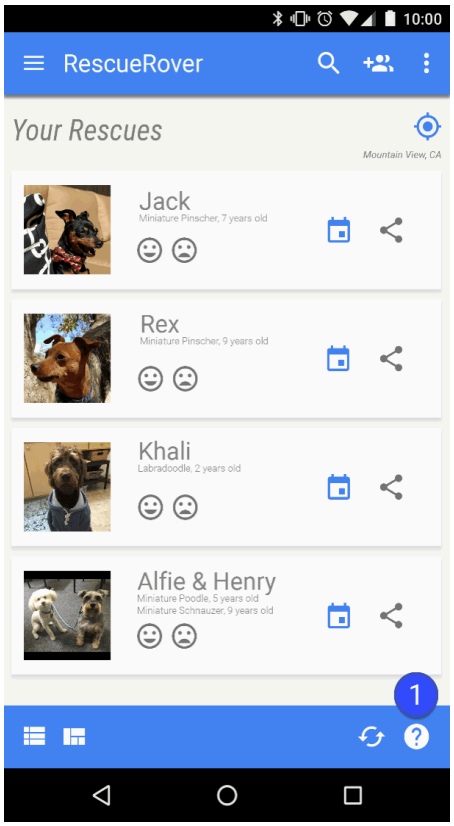
Se monetizzi un'app rivolta a bambini e ragazzi su Google Play, è importante che l'app sia conforme ai requisiti delle norme relative agli annunci e alla monetizzazione per le famiglie.

Annunci ingannevoli

Gli annunci non devono simulare o imitare l'interfaccia utente di funzionalità di app, come notifiche o elementi di avviso di un sistema operativo. All'utente deve essere chiaro in quale app è pubblicato ogni annuncio.

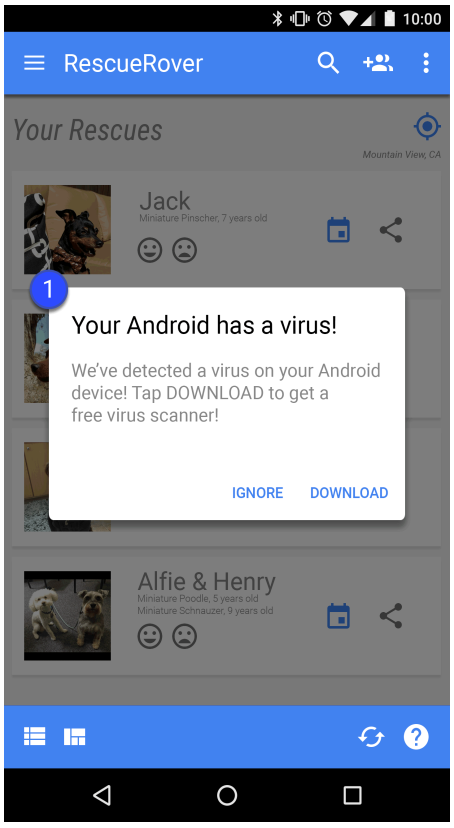
Di seguito sono riportati alcuni esempi di violazioni frequenti:

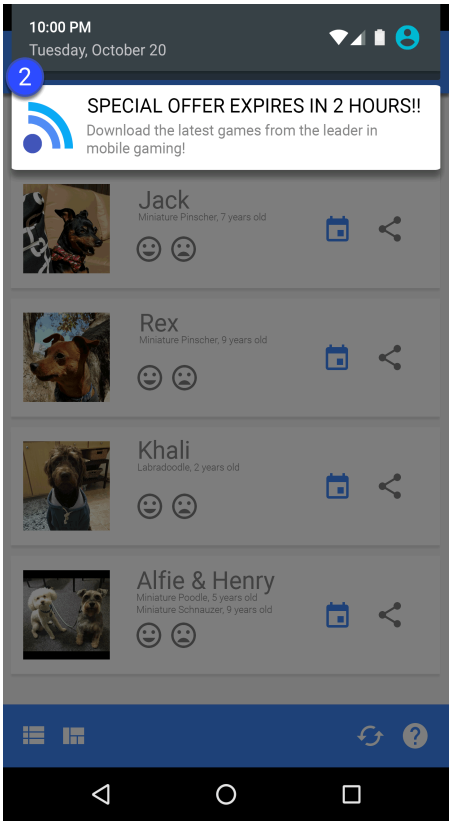
- Annunci che imitano l'interfaccia utente di un'app:



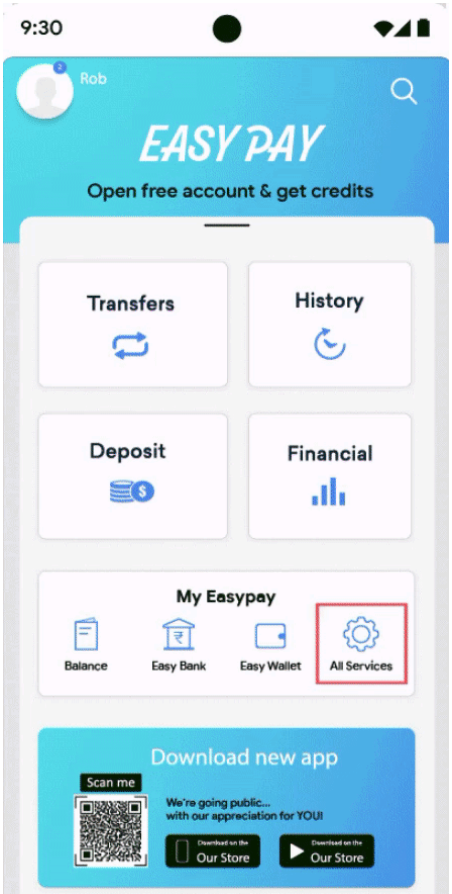
① L'icona a forma di punto interrogativo in questa app è un annuncio che rimanda l'utente a una pagina di destinazione esterna.

- Annunci che imitano una notifica di sistema:





① ② Gli esempi in alto mostrano annunci che imitano diverse notifiche di sistema.



① L'esempio in alto mostra una sezione di funzionalità che imita altre funzionalità e che in realtà rimanda soltanto l'utente a uno o più annunci.

Annunci improvvisi

Gli annunci improvvisi sono annunci che vengono mostrati agli utenti in modi imprevisti, che potrebbero generare clic involontari, compromettere l'usabilità delle funzionalità del dispositivo o interferire con questa.

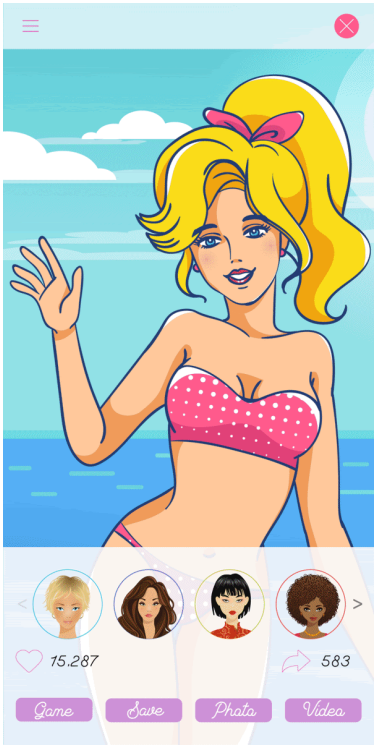
L'app non può obbligare un utente a fare clic su un annuncio o a inviare informazioni personali a scopi pubblicitari come condizione per poter utilizzare la funzionalità completa di un'app. Gli annunci possono essere mostrati solo all'interno dell'app che li pubblica e non devono interferire con altre app, altri annunci o con il funzionamento del dispositivo, inclusi pulsanti e porte del sistema o del dispositivo. Sono compresi overlay, funzionalità di supporto e unità pubblicitarie con widget. Se nell'app vengono mostrati annunci che interferiscono con il normale utilizzo, gli utenti devono poter ignorare facilmente gli annunci senza subire conseguenze negative.

Di seguito sono riportati alcuni esempi di violazioni frequenti:

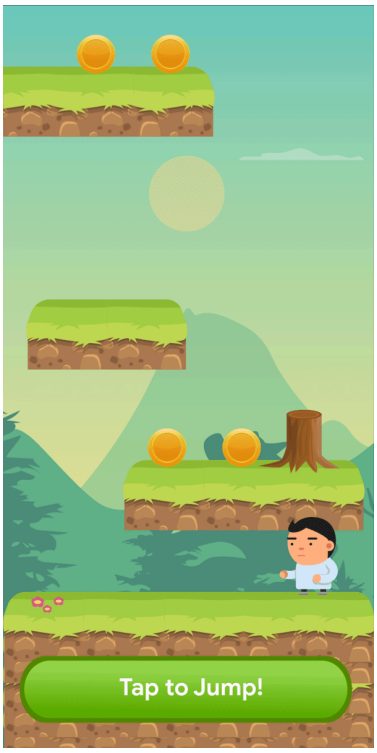
- Annunci che occupano tutto lo schermo o che interferiscono con il normale utilizzo, che non è chiaro come poter ignorare:

① Non è disponibile un pulsante per ignorare questo annuncio.

- Annunci che obbligano l'utente a eseguire il click-through usando un falso pulsante Ignora o facendo apparire improvvisamente gli annunci in aree dell'app che in genere l'utente tocca per accedere a un'altra funzionalità:

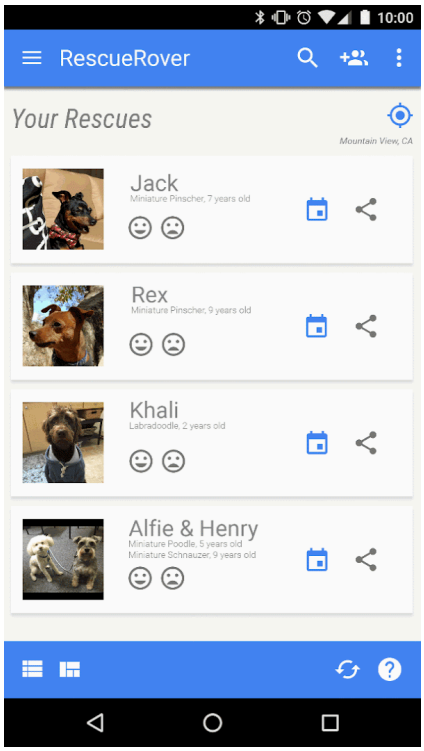


① Questo annuncio utilizza un falso pulsante Chiudi.



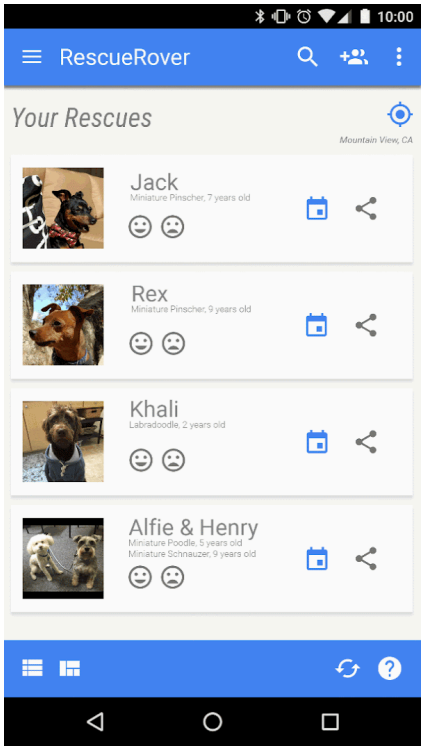
② Questo annuncio appare all'improvviso in un'area che l'utente è abituato a toccare per accedere alle funzioni in-app.

- Annunci che vengono mostrati all'esterno dell'app in cui sono pubblicati:



① L'utente passa alla schermata Home dell'app e compare all'improvviso un annuncio.

- Annunci che vengono attivati dal pulsante Home o da altre funzionalità progettate espressamente per uscire dall'app:



① L'utente cerca di uscire dall'app e di accedere alla schermata Home, ma il flusso previsto viene interrotto da un annuncio.

Esperienze di Better Ads

Gli sviluppatori sono tenuti a rispettare le seguenti linee guida per gli annunci per garantire esperienze di alta qualità agli utenti che usano le app di Google Play. Sono vietate, in quanto impreviste per gli utenti, le seguenti modalità di visualizzazione degli annunci:

- Gli annunci interstitial a schermo intero di tutti i formati (video, GIF, statici e così via) che vengono mostrati in modo imprevisto, tipicamente quando l'utente ha scelto di fare qualcos'altro.
  - Gli annunci che vengono mostrati nel gameplay all'inizio di un livello o di un segmento di contenuti.
  - Gli annunci interstitial a schermo intero che vengono visualizzati prima della schermata di caricamento (schermata iniziale) di un'app.
- Gli annunci interstitial a schermo intero di tutti i formati che non possono essere chiusi dopo 15 secondi. Gli interstitial a schermo intero ad attivazione o gli interstitial a schermo intero che non interrompono le azioni degli utenti (ad esempio, quelli visualizzati dopo la schermata dei punteggi nell'app di un gioco) possono essere visualizzati per più di 15 secondi.

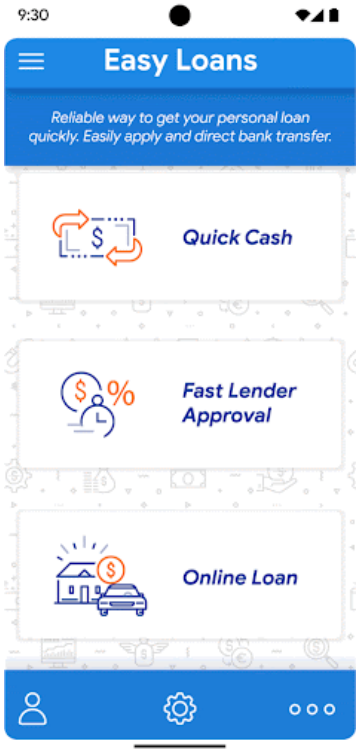
Queste norme non riguardano gli annunci con premio che vengono attivati esplicitamente dagli utenti (ad esempio un annuncio che gli sviluppatori offrono esplicitamente a un utente di guardare in cambio dello sblocco di una funzionalità o di un contenuto specifico di un gioco). Inoltre, queste norme non riguardano la monetizzazione e la pubblicità che non interferiscono con il normale uso dell'app o con il gameplay (ad esempio i contenuti video con annunci integrati e gli annunci banner non a schermo intero).

Queste linee guida si ispirano alle linee guida di Esperience di Better Ads . Per ulteriori informazioni su Better Ads Standards, consulta la pagina Coalition for Better Ads .

Di seguito sono riportati alcuni esempi di violazioni frequenti:

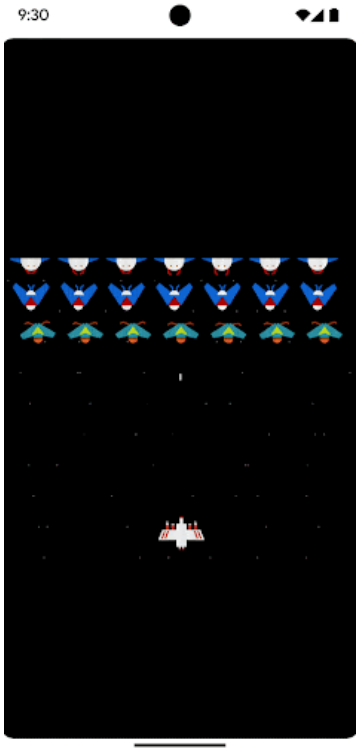
- Annunci imprevisti che vengono visualizzati durante il gameplay o all'inizio di un segmento di contenuti (ad esempio dopo che un utente ha fatto clic su un pulsante e prima che venga svolta l'azione prevista dal clic del pulsante). Questi annunci sono imprevisti per gli utenti, che si aspettano invece di iniziare un gioco o accedere a un contenuto.

① L'annuncio statico imprevisto viene visualizzato durante il gameplay all'inizio di un livello.



② L'annuncio video imprevisto viene visualizzato all'inizio di un segmento di contenuti.

- Un annuncio a schermo intero che viene visualizzato durante il gameplay e non può essere chiuso dopo 15 secondi.



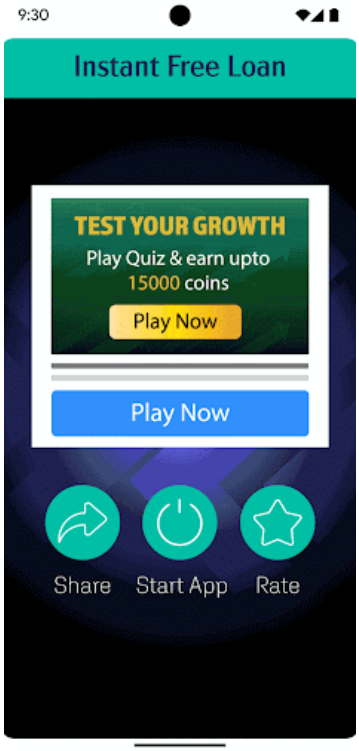
① Un annuncio interstitial viene visualizzato durante il gameplay e non offre all'utente la possibilità di ignorarlo dopo 15 secondi.

App realizzate appositamente per gli annunci

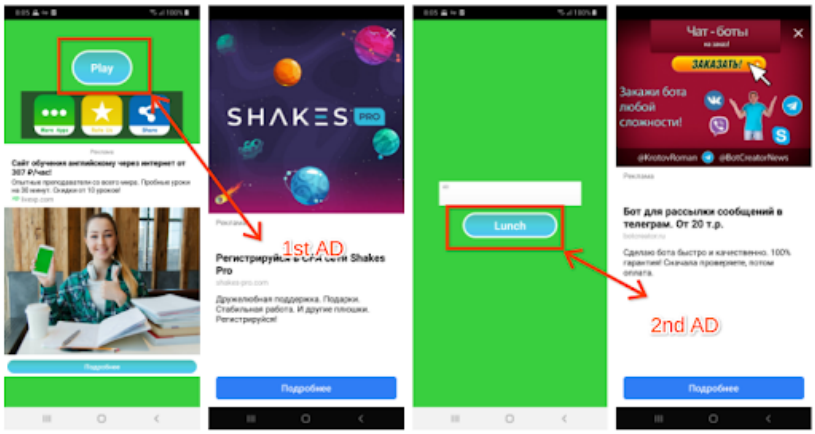
Sono vietate le app che mostrano ripetutamente annunci interstitial display in quanto distraggono gli utenti dall'interazione con l'app e dall'esecuzione delle attività nell'app.

Di seguito sono riportati alcuni esempi di violazioni frequenti:

- App in cui un annuncio interstitial è posizionato senza soluzione di continuità rispetto a un'azione dell'utente (inclusi, a titolo esemplificativo, clic, scorrimenti e così via).



① La prima pagina dell'app ha più pulsanti con cui è possibile interagire. Quando l'utente fa clic su **Avvia app** per usare l'app, viene mostrato un annuncio interstitial tramite popup. In seguito alla chiusura dell'annuncio, l'utente torna all'app e fa clic su **Servizio** per iniziare a usare il servizio, ma viene visualizzato un altro annuncio interstitial.



② Nella prima pagina l'utente è portato a fare clic su **Gioca** perché è l'unico pulsante disponibile per usare l'app. Quando l'utente fa clic sul pulsante, viene mostrato un annuncio interstitial. In seguito alla chiusura dell'annuncio, l'utente fa clic su **Avvia** perché è l'unico pulsante con cui è possibile interagire e viene visualizzato un altro annuncio interstitial tramite popup.

Monetizzazione della schermata di blocco

A meno che un'app non abbia esclusivamente la funzione di schermata di blocco, non devono esserci annunci o funzionalità che monetizzano la schermata di blocco di un dispositivo.

Frode pubblicitaria

La frode pubblicitaria è severamente vietata. Per ulteriori informazioni, consulta le norme relative alla frode pubblicitaria.

Utilizzo dei dati sulla posizione per gli annunci

Le app che estendono l'utilizzo dei dati sulla posizione del dispositivo basati sull'autorizzazione per la pubblicazione di annunci sono soggette alle norme relative a Informazioni personali e dati sensibili e devono inoltre soddisfare i seguenti requisiti:

- L'utilizzo o la raccolta per scopi pubblicitari di dati sulla posizione del dispositivo basati sull'autorizzazione devono essere chiari all'utente e documentati nelle norme sulla privacy obbligatorie dell'app, incluso il collegamento a eventuali norme sulla privacy di reti pubblicitarie pertinenti, relative all'utilizzo dei dati sulla posizione.
- In base ai requisiti relativi alle Autorizzazioni di accesso alla posizione, tali autorizzazioni possono essere richieste esclusivamente per implementare funzionalità o servizi esistenti nell'app e non è possibile richiedere autorizzazioni di accesso alla posizione del dispositivo esclusivamente per l'uso di annunci.

Utilizzo dell'ID pubblicità di Android

Nella versione 4.0 di Google Play Services sono state introdotte nuove API e un ID a disposizione dei fornitori di pubblicità e analisi. Di seguito sono riportati i termini per l'utilizzo dell'ID.

- **Utilizzo**. L'identificatore pubblicità di Android (AAID) deve essere utilizzato soltanto per la pubblicità e l'analisi degli utenti. A ogni accesso dell'ID è necessario verificare lo stato dell'impostazione di disattivazione della pubblicità basata sugli interessi o della personalizzazione degli annunci.
- **Associazione con informazioni che consentono l'identificazione personale o altri identificatori**.
  - Utilizzo pubblicitario: l'identificatore pubblicità non può essere collegato a identificatori del dispositivo persistenti (ad esempio SSAID, indirizzo MAC, IMEI e così via) per scopi pubblicitari. L'identificatore pubblicità può essere collegato a informazioni che consentono l'identificazione personale solo con il consenso esplicito dell'utente.
  - Utilizzo per scopi di analisi: l'identificatore pubblicità non può essere collegato a informazioni che consentono l'identificazione personale o associato a un identificatore del dispositivo persistente (ad esempio SSAID, indirizzo MAC, IMEI e così via) per scopi di analisi. Leggi le norme relative ai dati utente per ulteriori linee guida sugli identificatori del dispositivo persistenti.
- **Rispetto delle scelte degli utenti**.
  - In caso di reimpostazione, il nuovo identificatore pubblicità non deve essere collegato a un identificatore pubblicità precedente o a dati derivanti da un identificatore pubblicità precedente senza l'esplicito consenso dell'utente.
  - Devi rispettare l'impostazione di disattivazione della pubblicità basata sugli interessi o della personalizzazione degli annunci configurata dall'utente. Se un utente ha attivato questa impostazione, non puoi utilizzare l'identificatore pubblicità per creare profili utente per scopi pubblicitari o per eseguire il targeting degli utenti con pubblicità personalizzata. Sono ammessi, ad esempio, pubblicità contestuale, quota limite, monitoraggio delle conversioni, creazione di report e rilevamento di problemi di sicurezza e di attività fraudolente.
  - Sui dispositivi più recenti, quando un utente elimina l'identificatore pubblicità di Android, l'identificatore verrà rimosso. Qualsiasi tentativo di accesso all'identificatore restituirà una stringa di zeri. Un dispositivo privo di identificatore pubblicità non deve essere connesso ai dati collegati a un precedente identificatore pubblicità o da esso derivati.
- **Trasparenza per gli utenti**. La raccolta e l'utilizzo dell'identificatore pubblicità e l'impegno a rispettare i presenti termini devono essere comunicati agli utenti tramite una notifica in materia di privacy legalmente adeguata. Per ulteriori informazioni sui nostri standard per la privacy, consulta le norme relative ai dati utente .
- **Rispetto dei termini e condizioni d'uso**. L'identificatore pubblicità può essere utilizzato esclusivamente in conformità con le Norme del programma per gli sviluppatori di Google Play, anche dalle parti con cui tu lo condivida eventualmente nel corso della tua attività. Per tutte le app caricate

o pubblicate su Google Play è necessario utilizzare l'identificatore pubblicità (se disponibile sul dispositivo) anziché qualsiasi altro identificatore del dispositivo per qualunque finalità pubblicitaria.

Per ulteriori informazioni, consulta le nostre norme relative ai dati utente.

Abbonamenti

In qualità di sviluppatore, devi evitare di fuorviare gli utenti in merito a servizi o contenuti in abbonamento offerti all'interno dell'app. È fondamentale includere comunicazioni chiare in tutte le promozioni in-app o nelle schermate iniziali. Sono vietate le app che sottopongono gli utenti a esperienze di acquisto ingannevoli o manipolatorie (inclusi abbonamenti o acquisti in-app).

La tua offerta deve essere trasparente. Questo significa, tra le altre cose, indicare esplicitamente i termini dell'offerta, il costo dell'abbonamento, la frequenza del ciclo di fatturazione e se sia necessario un abbonamento per usare l'app. Agli utenti non dovrebbe essere richiesta alcuna ulteriore azione per esaminare le informazioni.

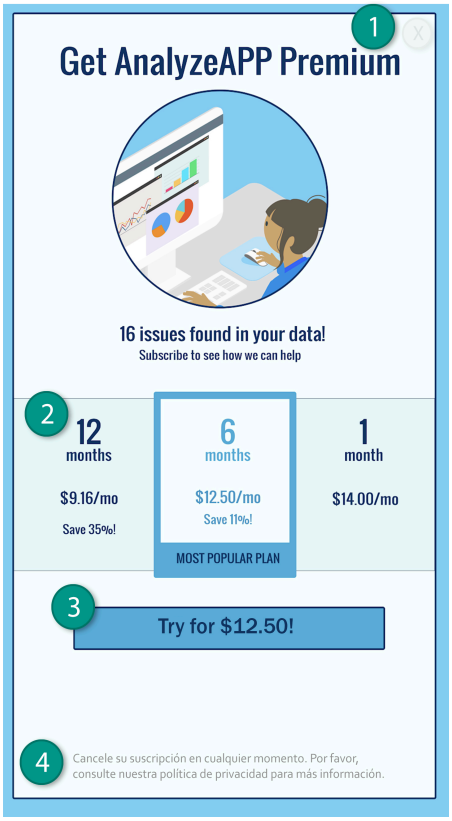
Gli abbonamenti devono fornire un valore ricorrente o costante agli utenti tramite la durata dell'abbonamento e non possono essere usati per offrire agli utenti vantaggi una tantum (ad esempio, SKU che offrono una forma di pagamento in crediti/valuta in-app o potenziamenti per i giochi da usare una sola volta). Il tuo abbonamento può offrire bonus promozionali o incentivi, ma questi devono essere complementari al valore ricorrente o costante fornito tramite la durata dell'abbonamento**.** I prodotti che non offrono un valore ricorrente o costante devono usare un prodotto in-app invece di un prodotto in abbonamento.

Non puoi camuffare o definire in modo errato i vantaggi una tantum come abbonamenti. È inclusa la modifica di un abbonamento affinché diventi un'offerta una tantum (ad esempio l'annullamento, il ritiro o la riduzione del valore ricorrente) dopo che l'utente ha acquistato l'abbonamento.

Di seguito sono riportati alcuni esempi di violazioni frequenti:

- Abbonamenti mensili che non informano gli utenti del fatto che il rinnovo sarà automatico e che l'addebito avverrà ogni mese.
- Abbonamenti annuali che evidenziano il prezzo in termini di costo mensile.
- Termini e prezzi dell'abbonamento localizzati in modo incompleto.
- Promozioni in-app che non spiegano chiaramente che l'utente può accedere ai contenuti anche senza abbonamento (quando disponibile).
- Nomi di SKU che non riflettono in modo accurato il tipo di abbonamento, ad esempio "Prova senza costi aggiuntivi" o "Prova l'abbonamento Premium: 3 giorni senza costi" per un abbonamento con addebito automatico per il rinnovo.
- Diverse schermate nel flusso di acquisto che portano gli utenti a fare clic in modo involontario sul pulsante Abbonati.
- Abbonamenti che non offrono un valore ricorrente o costante, ad esempio l'offerta di 1000 gemme il primo mese per poi ridurre il vantaggio a 1 gemma nei mesi seguenti dell'abbonamento.
- Registrazione obbligatoria da parte dell'utente a un abbonamento con rinnovo automatico per poter ottenere un vantaggio una tantum e annullamento dell'abbonamento di un utente senza che venga richiesto dopo l'acquisto.

Esempio 1:



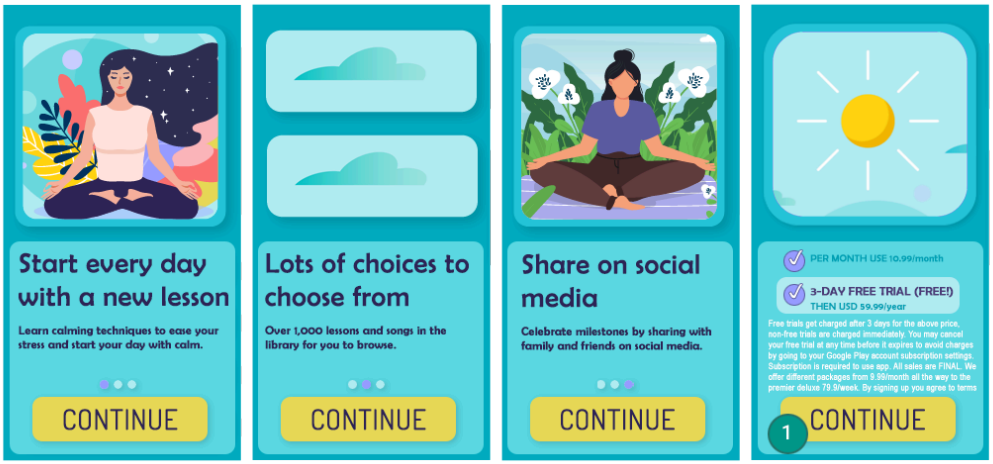
① Il pulsante Ignora non è chiaramente visibile e gli utenti potrebbero non comprendere che possono accedere alla funzionalità senza accettare l'offerta dell'abbonamento.

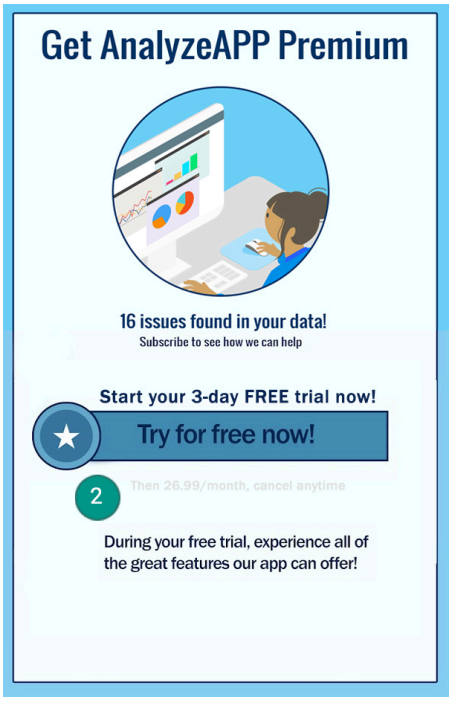
② Il prezzo dell'offerta viene visualizzato solo in termini di costo mensile e gli utenti potrebbero non comprendere che verrà addebitato loro il costo semestrale in un'unica soluzione al momento della sottoscrizione dell'abbonamento.

③ L'offerta mostra solo il prezzo di lancio e gli utenti potrebbero non comprendere quale importo verrà loro addebitato automaticamente al termine del periodo di lancio.

④ L'offerta deve essere localizzata nella stessa lingua dei termini e condizioni, in modo tale che gli utenti possano comprendere l'offerta nella sua totalità.

Esempio 2:





① Clic ricorrenti nella stessa area del pulsante potrebbero comportare il clic involontario da parte dell'utente sul pulsante "Continua" finale che consente di abbonarsi.

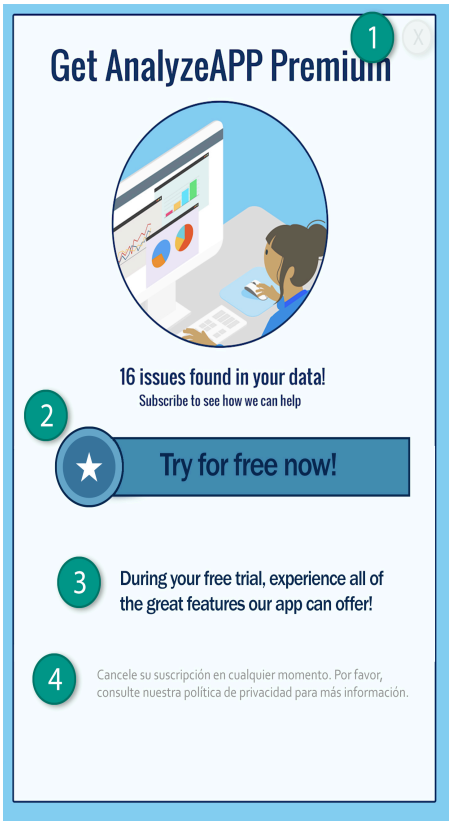
② L'importo che verrà addebitato agli utenti al termine della prova è poco leggibile, pertanto gli utenti potrebbero pensare che il piano sia senza costi.

Prove gratuite e offerte di lancio

Prima che un utente attivi l'abbonamento offerto dall'app: lo sviluppatore deve specificare in modo chiaro e preciso i termini della sua offerta includendo la durata, i prezzi e una descrizione dei contenuti o dei servizi accessibili. Lo sviluppatore deve assicurarsi di informare l'utente di quando e come una prova gratuita si convertirà in un abbonamento a pagamento, di quanto costerà tale abbonamento e del fatto che l'utente potrà annullare la prova gratuita qualora non voglia che si converta in un abbonamento a pagamento.

Di seguito sono riportati alcuni esempi di violazioni frequenti:

- Offerte che non spiegano chiaramente quanto durerà la prova gratuita o il prezzo di lancio.
- Offerte che non spiegano chiaramente che, al termine del periodo dell'offerta, per l'utente verrà automaticamente attivato un abbonamento a pagamento.
- Offerte che non spiegano chiaramente che l'utente può accedere ai contenuti senza una prova (quando disponibile).
- Prezzi e termini dell'offerta localizzati in modo incompleto.



① Il pulsante Ignora non è chiaramente visibile e gli utenti potrebbero non comprendere che possono accedere alla funzionalità senza iscriversi alla prova gratuita.

② L'offerta mette in evidenza la prova gratuita e gli utenti potrebbero non comprendere che alla fine del periodo di prova verrà effettuato un addebito a loro carico.

③ L'offerta non specifica il periodo di prova e gli utenti potrebbero non comprendere per quanto tempo durerà il loro accesso gratuito ai contenuti in abbonamento.

④ L'offerta deve essere localizzata nella stessa lingua dei termini e condizioni, in modo tale che gli utenti possano comprendere l'offerta completa.

Gestione degli abbonamenti, annullamento e rimborsi

Se vendi abbonamenti nella tua app o nelle tue app, devi assicurarti che comunichino chiaramente in che modo l'utente può gestire o annullare il proprio abbonamento. Inoltre, nell'app devi includere l'accesso a un metodo online facile da usare per annullare l'abbonamento. Nelle impostazioni dell'account della tua app (o nella pagina equivalente), puoi soddisfare i requisiti includendo:

- Un link al Centro abbonamenti di Google Play (per le app che usano il sistema di fatturazione di Google Play); e/o
- L'accesso diretto alla procedura di annullamento.

Se un utente annulla un abbonamento acquistato mediante il sistema di fatturazione di Google Play, le norme generali di Google prevedono che l'utente non riceva un rimborso per il periodo di fatturazione corrente, ma che continui a ricevere i contenuti in abbonamento per il resto di tale periodo di fatturazione a prescindere dalla data dell'annullamento. L'annullamento da parte dell'utente diventa valido al termine del periodo di fatturazione corrente.

In qualità di fornitore dei contenuti o dell'accesso, puoi implementare norme sui rimborsi più flessibili direttamente con i tuoi utenti. È tua responsabilità informare gli utenti in merito a eventuali modifiche apportate alle norme su abbonamento, annullamento e rimborsi e assicurarti che tali norme siano conformi alla legge vigente.

Programma relativo all'SDK per gli annunci autocertificati per la famiglia

Se pubblichi annunci nella tua app e il relativo pubblico di destinazione è costituito unicamente da bambini e ragazzi come descritto nelle Norme per le famiglie , devi utilizzare soltanto versioni dell'SDK per gli annunci che dispongono dell'autocertificazione di conformità con le norme di Google Play, inclusi i requisiti dell'SDK per gli annunci autocertificati per la famiglia che seguono.

Se il pubblico di destinazione dell'app include sia bambini e ragazzi sia utenti più adulti, devi assicurarti che gli annunci mostrati a bambini e ragazzi provengano esclusivamente da una di queste versioni dell'SDK per gli annunci autocertificati (ad esempio adottando misure quali il filtro di controllo dell'età).

Tieni presente che è tua responsabilità garantire che tutte le versioni dell'SDK implementate nell'app (incluse le versioni dell'SDK per gli annunci autocertificati) siano conformi a tutte le norme, leggi locali e normative vigenti. Google non fornisce alcuna dichiarazione o garanzia in merito all'esattezza delle informazioni fornite dagli SDK per gli annunci durante la procedura di autocertificazione.

L'utilizzo di SDK per gli annunci autocertificati per la famiglia è richiesto solo se usi gli SDK per gli annunci per mostrare annunci ai bambini. Quanto indicato di seguito è consentito senza obbligo di autocertificazione dell'SDK per gli annunci con Google Play, ma rimani responsabile di garantire che i contenuti degli annunci e le procedure di raccolta dei dati siano conformi alle norme relative ai dati utente e alle Norme per le famiglie di Google Play:

- Pubblicità autopromozionale qualora tu utilizzi SDK per gestire la promozione incrociata delle tue app o per altri media e merchandising di proprietà.
- Conclusione di direct deal con gli inserzionisti qualora tu utilizzi SDK per la gestione dell'inventario.

Requisiti relativi all'SDK per gli annunci autocertificati per la famiglia

- Definisci i contenuti degli annunci e i comportamenti discutibili e vietali nei termini o nelle norme dell'SDK per gli annunci. Le definizioni devono essere conformi alle Norme del programma per gli sviluppatori di Google Play.
- Crea un metodo per classificare le creatività degli annunci in base alle fasce d'età appropriate. Queste ultime devono includere almeno le fasce Per tutti e Per adulti. La metodologia di classificazione deve essere in linea con la metodologia che Google fornisce agli SDK una volta che gli sviluppatori abbiano compilato il modulo di interesse riportato di seguito.
- Consenti ai publisher, in base alle singole richieste o per app, di richiedere un trattamento per siti o servizi destinati ai minori per la pubblicazione di annunci. Questo trattamento deve essere conforme alle leggi e normative vigenti, come la legge statunitense Children's Online Privacy Protection Act (COPPA) e il Regolamento generale sulla protezione dei dati (GDPR) dell'UE . Google Play richiede che gli SDK per gli annunci disattivino annunci personalizzati, pubblicità basata sugli interessi e remarketing nell'ambito del trattamento per siti o servizi destinati ai minori.
- Consenti ai publisher di selezionare formati degli annunci conformi alle norme relative agli annunci e alla monetizzazione per le famiglie di Google Play e che soddisfino i requisiti del programma App approvate dagli insegnanti .
- Assicurati che, quando le offerte in tempo reale vengono utilizzate per mostrare annunci a bambini e ragazzi, le creatività siano state esaminate e gli indicatori relativi alla privacy vengano applicati agli offerenti.
- Fornisci a Google informazioni sufficienti, ad esempio inviando un'app di prova e fornendo le informazioni indicate nel modulo di interesse riportato di seguito, per verificare la conformità dell'SDK per gli annunci a tutti i requisiti di autocertificazione. Inoltre, rispondi tempestivamente a eventuali richieste successive di informazioni, ad esempio di invio di nuove versioni per verificare la conformità della versione dell'SDK per gli annunci a tutti i requisiti di certificazione, nonché di fornitura di un'app di prova.
- Autocertifica che tutte le nuove versioni siano conformi con le Norme del programma per gli sviluppatori di Google Play più recenti, inclusi i requisiti delle Norme per le famiglie.

Nota: gli SDK per gli annunci autocertificati per la famiglia devono supportare la pubblicazione di annunci in conformità con tutte le leggi e normative vigenti relative a bambini e ragazzi che possano applicarsi ai rispettivi publisher.

In questa pagina puoi trovare ulteriori informazioni sull'applicazione della filigrana alle creatività degli annunci e sulla fornitura di un'app di prova.

I requisiti di mediazione per le piattaforme di pubblicazione in caso di pubblicazione di annunci destinati a bambini e ragazzi sono i seguenti:

- Utilizza solo SDK per gli annunci autocertificati per la famiglia o implementa le misure di protezione necessarie per garantire che tutti gli annunci pubblicati dalle reti di mediazione siano conformi a questi requisiti; e
- Trasmetti le informazioni necessarie alle piattaforme di mediazione per indicare la classificazione dei contenuti degli annunci e l'eventuale trattamento applicabile per siti o servizi destinati ai minori.

In questa pagina gli sviluppatori possono consultare un elenco di SDK per gli annunci autocertificati per la famiglia e controllare quali versioni specifiche di questi SDK per gli annunci dispongono dell'autocertificazione per l'utilizzo in app per la famiglia.

Inoltre, gli sviluppatori possono condividere questo modulo di interesse con gli SDK per gli annunci che vorrebbero ottenere l'autocertificazione.

Scheda dello Store e promozione

La promozione e la visibilità delle app incidono notevolmente sulla qualità dello store. Evita schede dello store contenenti spam, promozioni di scarsa qualità e tentativi di aumentare in modo artificiale la visibilità delle app su Google Play.

Promozione di app

Sono vietate le app che adottano o beneficiano, direttamente o indirettamente, di pratiche di promozione (quali gli annunci) ingannevoli o dannose per gli utenti o per l'ecosistema degli sviluppatori. Le pratiche di promozione sono ingannevoli o dannose se il loro comportamento o i loro contenuti violano le nostre Norme del programma per gli sviluppatori.

Di seguito sono riportati alcuni esempi di violazioni frequenti:

- Utilizzo di annunci ingannevoli su siti web, app o altre proprietà, incluse notifiche simili ad avvisi e notifiche di sistema.
- Utilizzo di annunci sessualmente espliciti per indirizzare gli utenti alla scheda di Google Play della tua app per il download.
- Tecniche di promozione o installazione che reindirizzano gli utenti a Google Play o al download di app senza un'azione informata da parte dell'utente.
- Promozione non richiesta tramite servizi SMS.
- Titolo, icona o nome dello sviluppatore dell'app contenenti testo o immagini che indicano le prestazioni o il ranking sullo store, includono prezzi o informazioni promozionali oppure suggeriscono collegamenti con programmi di Google Play esistenti.

È tua responsabilità assicurarti che qualsiasi rete pubblicitaria, società consociata o annuncio associati alla tua app rispettino queste norme.

Metadati

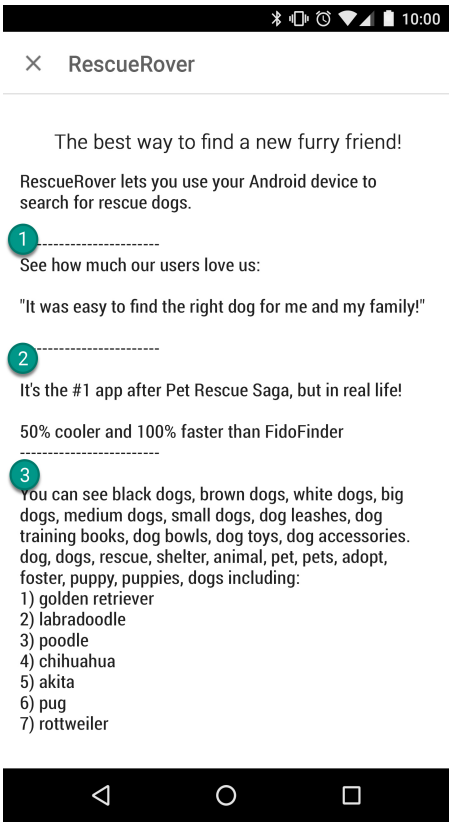
Gli utenti si affidano alle descrizioni dell'app per comprenderne la funzionalità e lo scopo. Sono vietate le app contenenti metadati fuorvianti, non correttamente formattati, non descrittivi, irrilevanti, eccessivi o inappropriati che siano contenuti, a titolo esemplificativo ma non esaustivo, nella

descrizione, nel nome sviluppatore, nel titolo, nell'icona, negli screenshot e nelle immagini promozionali dell'app. Gli sviluppatori sono tenuti a fornire una descrizione chiara e ben scritta della loro app. Inoltre nella descrizione dell'app non sono consentite testimonianze degli utenti prive di attribuzione o anonime.

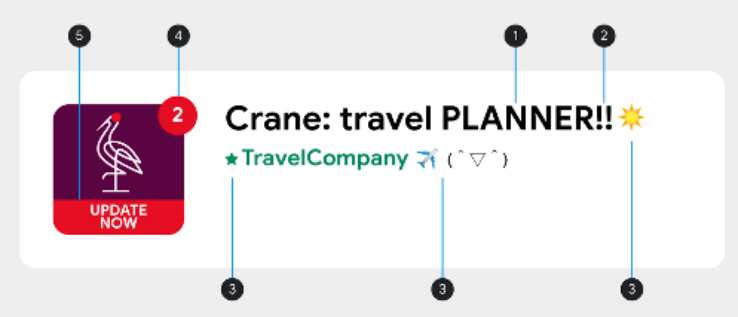
Il titolo e l'icona dell'app, nonché il nome dello sviluppatore, sono particolarmente utili per consentire agli utenti di trovare la tua app e acquisire informazioni in merito. Non usare emoji, emoticon o caratteri speciali ripetuti in questi elementi dei metadati. Evita di usare parole TUTTE MAIUSCOLE, a meno che non facciano parte del nome del brand. Sono vietati simboli ingannevoli nelle icone delle app, ad esempio: pallino che indica la presenza di nuovi messaggi quando in realtà non ce ne sono e simboli di download/installazione quando l'app non è correlata al download di contenuti. Il titolo dell'app deve contenere massimo 30 caratteri. Il titolo, l'icona o il nome dello sviluppatore dell'app non devono contenere testo o immagini che indichino le prestazioni o il ranking sullo store, includano prezzi o informazioni promozionali oppure suggeriscano collegamenti con programmi di Google Play esistenti.

Oltre ai requisiti qui indicati, norme per gli sviluppatori di Google Play specifiche potrebbero richiedere di fornire ulteriori informazioni nei metadati.

Di seguito sono riportati alcuni esempi di violazioni frequenti:

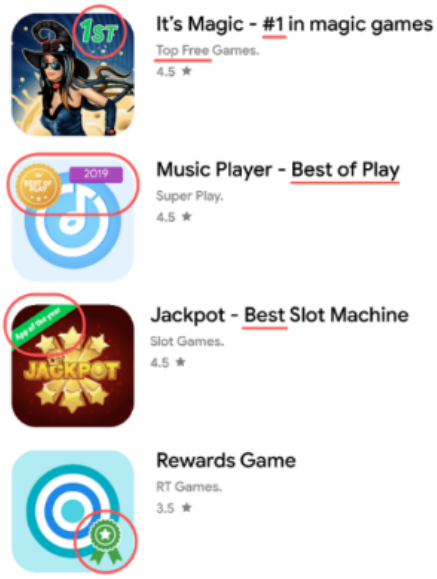


① Testimonianze degli utenti anonime o non attribuite
② Confronti di dati di app o brand
③ Blocchi di parole ed elenchi di parole verticali oppure orizzontali

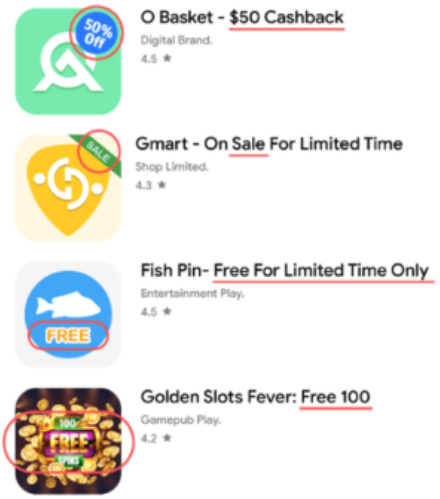


① Parole TUTTE MAIUSCOLE che non fanno parte del nome del brand
② Sequenze di caratteri speciali irrilevanti per l'app
③ Uso di emoji, emoticon (anche kaomoji) e caratteri speciali
④ Simbolo ingannevole
⑤ Testo ingannevole

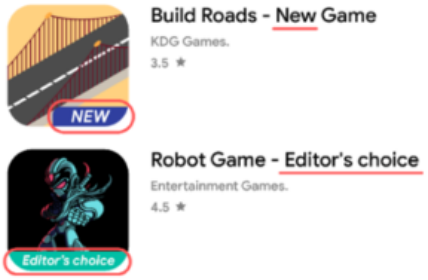
- Immagini o testo che indichino le prestazioni o il ranking sullo store, ad esempio "App dell'anno", "N. 1," "Migliore app su Google Play 20XX", "Popolare", icone di premi e così via.



- Immagini o testo che indichino informazioni promozionali e sul prezzo, ad esempio "Sconto del 10%", "Cashback di 50 $", "gratis per un periodo limitato" e così via.



- Immagini o testo che indichino programmi di Google Play, ad esempio "Da non perdere", "Novità" e così via.



Di seguito sono riportati alcuni esempi di testo, immagini o video inappropriati presenti nella tua scheda:

- Immagini o video con contenuti a sfondo sessuale. Evita di utilizzare immagini allusive che mostrino seni, natiche, genitali o altre parti anatomiche o contenuti oggetto di feticismo, sia illustrati sia reali.
- Utilizzo di linguaggio volgare o comunque non appropriato per un pubblico generico nella scheda dello Store dell'app.
- Violenza esplicita mostrata in evidenza nelle icone delle app, nelle immagini promozionali o nei video.
- Raffigurazioni dell'utilizzo illegale di droghe. Anche i contenuti a scopo didattico, documentaristico, scientifico o artistico devono essere adatti a tutti i tipi di pubblico all'interno della scheda dello Store.

Di seguito sono riportate alcune best practice:

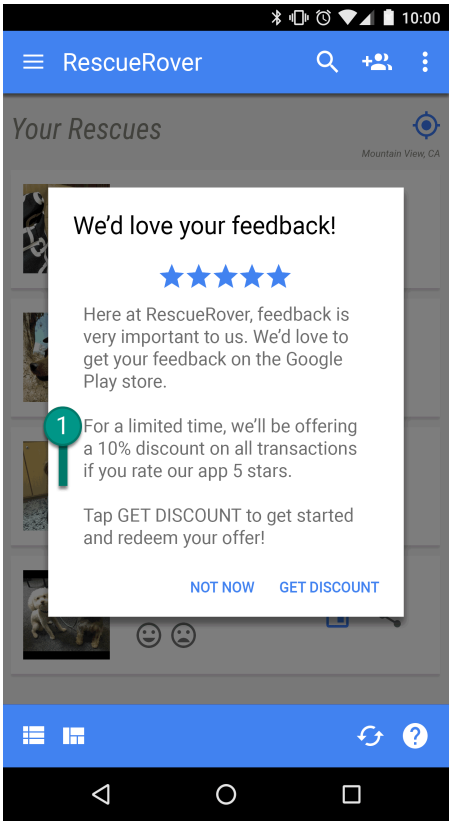
- Evidenzia gli aspetti migliori della tua app. Condividi con gli utenti fatti interessanti e coinvolgenti relativi alla tua app per aiutarli a capire che cosa la rende speciale.
- Assicurati che il titolo e la descrizione dell'app ne illustrino in modo accurato la funzionalità.
- Evita di utilizzare parole chiave o riferimenti ripetitivi o estranei al contesto.
- La descrizione dell'app deve essere breve e diretta. Le descrizioni brevi tendenzialmente offrono un'esperienza utente migliore, in particolare sui dispositivi con schermi piccoli. Lunghezza o dettagli eccessivi, formattazione non valida o ripetizioni potrebbero costituire una violazione di queste norme.
- Tieni presente che la scheda deve essere adatta a un pubblico generico. Evita di utilizzare testo, immagini o video inappropriati nella scheda e attieniti alle linee guida riportate in precedenza.

Valutazioni, recensioni e installazioni degli utenti

Gli sviluppatori non devono tentare di manipolare il posizionamento di qualsiasi app in Google Play. È vietato quindi, a titolo esemplificativo ma non esaustivo, incrementare artificialmente le valutazioni dei prodotti, le recensioni o il numero di installazioni con mezzi illeciti, ad esempio tramite recensioni e valutazioni fraudolente o influenzate dall'offerta di incentivi, nonché offrire app il cui scopo principale sia incentivare gli utenti a installare altre app.

Di seguito sono riportati alcuni esempi di violazioni frequenti:

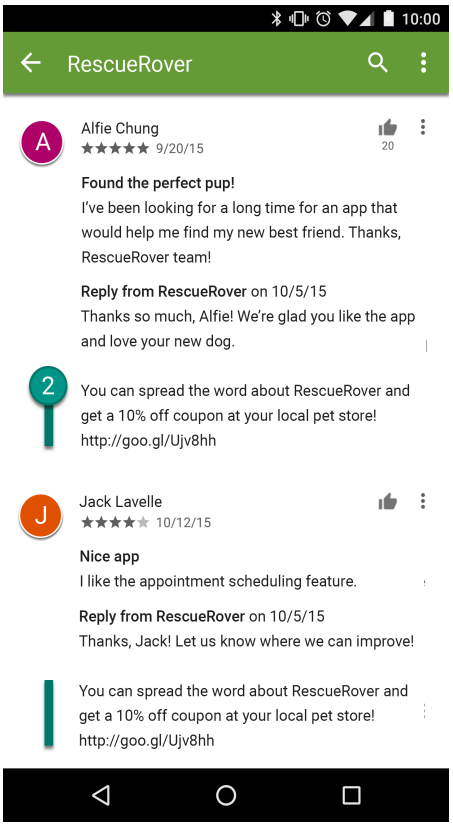
- Richiesta agli utenti di valutare l'app offrendo un incentivo:



① Questa notifica offre agli utenti uno sconto in cambio di una valutazione elevata.

- Invio a ripetizione di valutazioni fingendosi utenti per influenzare il posizionamento dell'app su Google Play.

- Invio o esortazione agli utenti a inviare recensioni con contenuti inappropriati, inclusi coupon, affiliazioni, codici di gioco, indirizzi email o link che rimandano a siti web o altre app:



② Questa recensione esorta gli utenti a promuovere l'app RescueRover offrendo in cambio un coupon.

Le valutazioni e le recensioni sono parametri di qualità delle app, e per gli utenti è fondamentale che siano autentici e pertinenti. Di seguito sono riportate alcune best practice da seguire per rispondere alle recensioni degli utenti:

- Mantieni la risposta focalizzata sui problemi sollevati nei commenti dell'utente e non richiedere una valutazione più alta.
- Includi riferimenti a risorse utili, ad esempio un indirizzo per l'assistenza o una pagina di domande frequenti.

Classificazioni dei contenuti

Le classificazioni dei contenuti su Google Play sono fornite dall'IARC (International Age Rating Coalition) e sono concepite per aiutare gli sviluppatori a comunicare agli utenti le classificazioni dei contenuti pertinenti a livello locale. Le autorità IARC regionali definiscono linee guida utilizzate per determinare il livello di maturità dei contenuti in un'app. Su Google Play non sono consentite app senza classificazione dei contenuti.

Modalità di utilizzo delle classificazioni dei contenuti

Le classificazioni dei contenuti vengono utilizzate per informare i consumatori, specialmente i genitori, riguardo ai contenuti potenzialmente discutibili presenti in un'app. Consentono inoltre di filtrare o bloccare i contenuti in determinati territori o per utenti specifici ove previsto dalla legge e determinare l'idoneità dell'app a programmi speciali per sviluppatori.

Modalità di assegnazione delle classificazioni dei contenuti

Per ricevere la classificazione dei contenuti, è necessario compilare un questionario per la classificazione in Play Console con domande sulla natura dei contenuti delle app. In base alle risposte al questionario, a ogni app verrà assegnata una classificazione dei contenuti da parte di più autorità di classificazione. La rappresentazione ingannevole dei contenuti delle app potrebbe comportarne la rimozione o la sospensione, perciò è importante dare risposte precise alle domande del questionario relativo alla classificazione dei contenuti.

Per evitare che un'app venga elencata come "Non classificata", è necessario compilare il questionario per la classificazione dei contenuti per ogni nuova app inviata alla Play Console e per tutte le app esistenti che sono attive su Google Play. Le app sprovviste di una classificazione dei contenuti verranno rimosse dal Play Store.

Se i contenuti o le funzionalità dell'app vengono modificati in modo tale da influire sulle risposte al questionario di classificazione, è necessario inviare un nuovo questionario relativo alla classificazione dei contenuti all'interno di Play Console.

Visita il Centro assistenza per ulteriori informazioni sulle diverse Autorità di classificazione e su come completare il questionario per la classificazione dei contenuti.

Ricorsi contro le classificazioni

Se non sei d'accordo con la classificazione assegnata alla tua app, puoi presentare un ricorso direttamente all'autorità di classificazione dell'IARC utilizzando il link disponibile nel certificato inviato via email.

Notizie

Un'app di notizie è un'app che:

- Si autodefinisce "di notizie" in Google Play Console oppure
- Si inserisce nella categoria "Notizie e riviste" del Google Play Store e si autodefinisce "di notizie" nel titolo, nell'icona, nel nome dello sviluppatore o nella descrizione

Ecco alcuni esempi di app nella categoria "Notizie e riviste" che possono essere considerate app di notizie:

- App che si autodefiniscono "di notizie" nelle relative descrizioni incluse, a titolo esemplificativo:
  - Notizie più recenti
  - Notizie di giornale
  - Ultime notizie
  - Notizie locali
  - Notizie del giorno
- App che includono la parola "notizie" nei titoli, nelle icone o nel nome dello sviluppatore

Tuttavia, le app che includono principalmente contenuti generati dagli utenti (ad esempio le app di social media) non devono autodefinirsi app di notizie e non vengono considerate tali.

Le app di notizie che richiedono agli utenti di acquistare un abbonamento devono fornire un'anteprima dei contenuti in-app prima dell'acquisto.

Le app di notizie devono:

- Dare informazioni sulla proprietà relative all'app e alla fonte degli articoli inclusi, a titolo esemplificativo, l'autore o l'editore originali di ogni articolo. Nei casi in cui non è consuetudine elencare i singoli autori degli articoli, l'app di notizie deve indicare l'editore originale degli articoli. Tieni presente che i link ad account di social media non sono considerati sufficienti come informazioni relative ad autori ed editori.
- Avere una pagina dedicata nell'app o nel sito web che indichi chiaramente di contenere dati di contatto, che sia facile da trovare (ad esempio tramite link nella parte inferiore della home page o nella barra di navigazione del sito) e che fornisca dati di contatto validi dell'editore giornalistico. Queste informazioni devono includere un indirizzo email o un numero di telefono di contatto. Tieni presente che i link ad account di social media non sono considerati sufficienti come dati di contatto degli editori.

Le app di notizie non devono:

- Contenere errori ortografici e/o grammaticali significativi
- Includere soltanto contenuti statici (ad esempio contenuti pubblicati più di tre mesi prima della data corrente) o
- Avere come finalità principale l'affiliate marketing o le entrate pubblicitarie

Tieni presente che le app di notizie *possono* usare annunci e altre forme di marketing per la monetizzazione, purché la finalità principale delle app non sia vendere prodotti e servizi o generare entrate pubblicitarie.

Le app di notizie che aggregano contenuti di diverse fonti editoriali devono essere trasparenti in merito alle fonti dei contenuti nell'app; ogni fonte deve rispettare i requisiti delle norme relative alle notizie.

Consulta questo articolo su come fornire al meglio le informazioni richieste.

Spam, funzionalità ed esperienza utente

Le app dovrebbero fornire agli utenti un livello base di funzionalità e contenuti adeguati per un'esperienza utente coinvolgente. Le app che hanno arresti anomali, presentano altri comportamenti

non in linea con un'esperienza utente funzionale o hanno il solo scopo di inviare spam agli utenti o inserire spam su Google Play non sono considerate app che contribuiscono al catalogo in modo costruttivo.

Spam

Sono vietate le app che inviano spam agli utenti o inseriscono spam su Google Play, ad esempio le app che inviano messaggi indesiderati agli utenti oppure le app duplicate o di scarsa qualità.

Messaggi spam

Sono vietate le app che inviano SMS, email o altri messaggi per conto dell'utente senza offrire a quest'ultimo la possibilità di verificare i contenuti e i destinatari previsti.

Di seguito è riportato un esempio di violazione frequente:

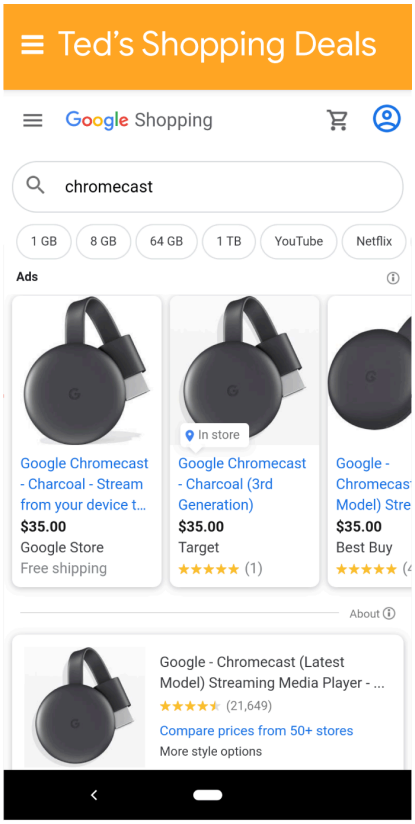
- Quando l'utente preme il pulsante "Condividi", l'app invia dei messaggi per conto dell'utente senza offrirgli la possibilità di confermare i contenuti né i destinatari previsti:

Spam legato alle visualizzazioni web e per promuovere traffico affiliato

Sono vietate le app il cui scopo principale è indirizzare traffico affiliato verso un sito web o fornire una visualizzazione web di un sito senza l'autorizzazione del proprietario o dell'amministratore del sito stesso.

Di seguito sono riportati alcuni esempi di violazioni frequenti:

- Un'app il cui scopo principale è indirizzare il traffico dai referral verso un sito web al fine di ricevere crediti per le registrazioni o gli acquisti degli utenti sul sito in questione.
- App il cui scopo principale è fornire una visualizzazione web di un sito web senza autorizzazione:



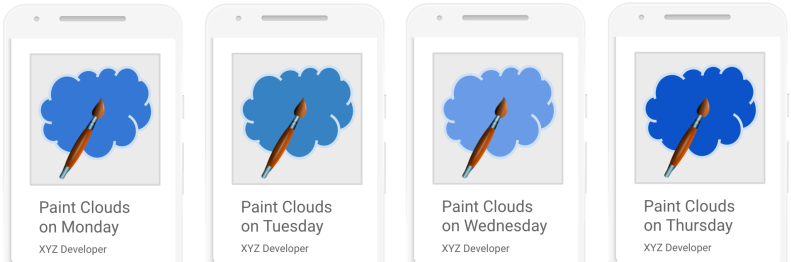
① Questa app è denominata "Ted's Shopping Deals" e fornisce semplicemente una visualizzazione web di Google Shopping.

Contenuti ripetitivi

Sono vietate le app che forniscono semplicemente la stessa esperienza di altre app già presenti su Google Play. Le app dovrebbero essere utili per gli utenti e quindi fornire servizi o contenuti unici.

Di seguito sono riportati alcuni esempi di violazioni frequenti:

- La copia di contenuti di altre app senza aggiungere alcun contenuto originale o alcuna utilità.
- Creazione di più app con funzionalità, contenuti ed esperienze utente molto simili. Se il volume di contenuti di ogni singola app è ridotto, gli sviluppatori dovrebbero valutare la creazione di un'app unica che raccolga tutti i contenuti.



Funzionalità, contenuti ed esperienza utente

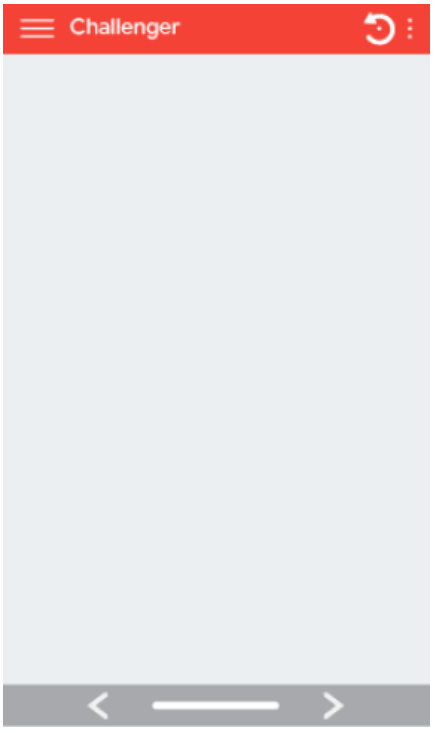
Le app dovrebbero fornire un'esperienza utente stabile, reattiva e coinvolgente. Su Google Play non sono consentite app che hanno arresti anomali, prive di un livello base di utilità adeguata in qualità di app mobile, prive di contenuti coinvolgenti o che presentano altri comportamenti non coerenti con un'esperienza utente funzionale e coinvolgente.

Funzionalità e contenuti limitati

Non sono consentite app con funzionalità e contenuti limitati.

Di seguito è riportato un esempio di violazione frequente:

- App statiche senza funzionalità specifiche, ad esempio app che contengono solo testo o file PDF
- App con pochissimi contenuti e che non offrono un'esperienza utente coinvolgente, ad esempio app che contengono solo uno sfondo
- App progettate per non fare nulla o per non avere alcuna funzione



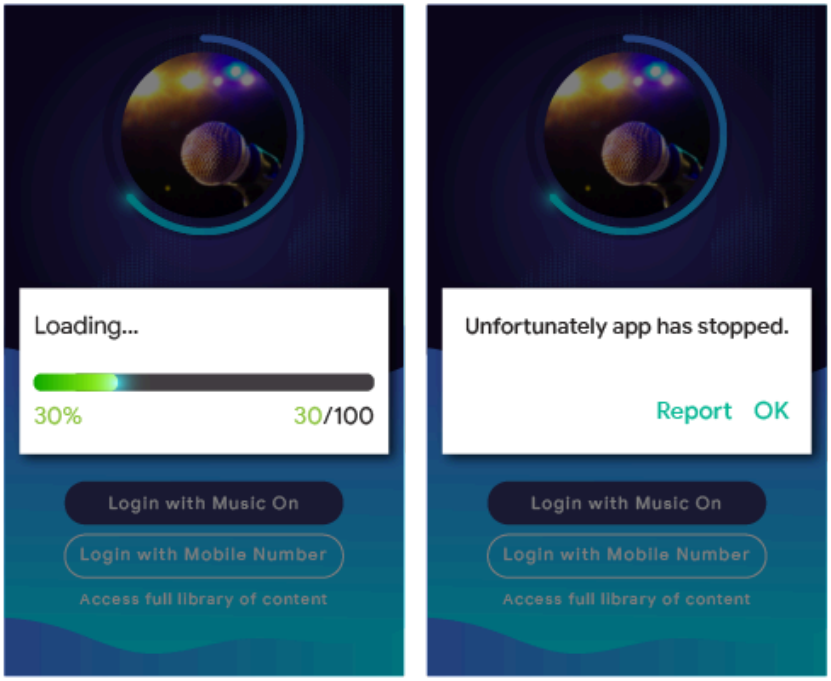
Funzioni inaccessibili

Sono vietate le app che si arrestano in modo anomalo, chiedono di forzare la chiusura, si bloccano o funzionano in maniera anomala.

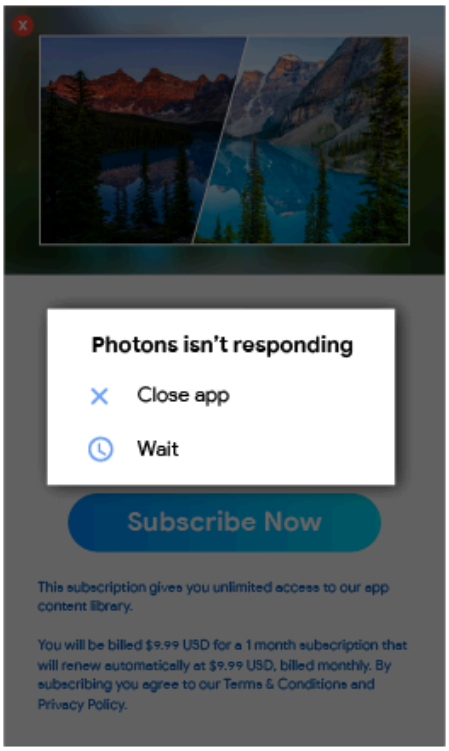
Di seguito sono riportati alcuni esempi di violazioni frequenti:

- App che **non si installano**

- App che si installano, ma **non si caricano**



- App che si caricano, ma **non sono reattive**



Altri programmi

Oltre a dover essere conformi alle norme relative ai contenuti stabilite altrove nel presente Centro norme, le app ideate per altre esperienze Android e distribuite tramite Google Play potrebbero anche

essere soggette a requisiti relativi alle norme specifici del programma. Assicurati di leggere l'elenco che segue per stabilire se ci sono delle norme che si applicano alla tua app.

App istantanee Android

Abbiamo realizzato le app istantanee Android con lo scopo di offrire agli utenti esperienze piacevoli e semplicissime rispettando allo stesso tempo gli standard più elevati di privacy e sicurezza. Le nostre norme sono state pensate a sostegno di tale scopo.

Gli sviluppatori che scelgono di distribuire app istantanee Android tramite Google Play devono rispettare le norme che seguono, oltre a tutte le altre Norme del programma di Google Play per gli sviluppatori.

Identità

Gli sviluppatori di app istantanee con funzionalità di accesso devono integrare la funzione Smart Lock per password .

Supporto dei link

Gli sviluppatori di app istantanee Android sono tenuti a supportare correttamente i link relativi ad altre app. Se le app installate o le app istantanee dello sviluppatore contengono link che potrebbero rimandare a un'app istantanea, lo sviluppatore deve indirizzare gli utenti a tale app anziché, ad esempio, mostrare i link in un componente WebView .

Specifiche tecniche

Gli sviluppatori devono rispettare le specifiche tecniche e i requisiti relativi alle app istantanee Android (che potrebbero essere occasionalmente modificati) indicati da Google, inclusi quelli riportati nella nostra documentazione pubblica .

Offerta dell'installazione di app

L'app istantanea potrebbe offrire all'utente l'app installabile, ma questo non deve essere lo scopo principale dell'app istantanea. Se offre l'installazione, gli sviluppatori sono tenuti a:

- Usare l'icona "get app" (scarica l'app) di Material Design e l'etichetta "Installa" per il pulsante di installazione.
- Non avere più di due o tre richieste di installazione implicite nell'app istantanea.
- Non usare un banner o un'altra tecnica in stile pubblicitario per presentare una richiesta di installazione agli utenti.

Ulteriori dettagli sulle app istantanee e linee guida relative all'esperienza utente sono disponibili nella pagina contenente le best practice per l'esperienza utente .

Modifica dello stato del dispositivo

Le app istantanee non devono apportare al dispositivo dell'utente modifiche che permangano più a lungo della sessione con l'app istantanea. Ad esempio, le app istantanee non possono cambiare lo sfondo dell'utente o creare un widget nella schermata Home.

Visibilità delle app

Gli sviluppatori devono assicurarsi che le app istantanee siano visibili all'utente in modo che quest'ultimo sia sempre a conoscenza dell'esecuzione dell'app sul proprio dispositivo.

Identificatori dei dispositivi

Le app istantanee non sono autorizzate ad accedere agli identificatori dei dispositivi che (1) persistono dopo l'interruzione dell'esecuzione dell'app istantanea e (2) non sono reimpostabili dall'utente. Di seguito sono riportati alcuni esempi:

- Numero di serie della build
- Indirizzi MAC di chip di rete
- IMEI, IMSI

Le app istantanee potrebbero accedere al numero di telefono se ottenuto usando l'autorizzazione relativa al tempo di esecuzione. Lo sviluppatore non deve cercare di identificare l'utente usando questi identificatori o qualsiasi altro mezzo.

Traffico di rete

Il traffico di rete dall'interno dell'app istantanea deve essere criptato usando un protocollo TLS come HTTPS.

Norme Android relative alle emoji

Le nostre norme relative alle emoji sono state pensate per promuovere un'esperienza utente inclusiva e uniforme. Per questo motivo, tutte le app installate su Android 12 o versioni successive devono supportare l'ultima versione di Unicode Emoji .

Le app installate su Android 12 o versioni successive che usano emoji Android predefinite senza implementazioni personalizzate usano già l'ultima versione di Unicode Emoji.

Le app installate su Android 12 o versioni successive con implementazioni di emoji personalizzate, incluse quelle fornite da librerie di terze parti, devono supportare completamente l'ultima versione Unicode entro 4 mesi dal rilascio della nuova versione di Unicode Emoji.

Consulta questa guida per avere informazioni su come supportare le emoji moderne.

Famiglie

Google Play offre agli sviluppatori una piattaforma completa per mostrare contenuti di alta qualità, adatti alle specifiche fasce d'età e idonei per tutta la famiglia. Prima di inviare un'app per il programma Per la famiglia o presentare un'app destinata ai bambini sul Google Play Store, hai la responsabilità di assicurarti che l'app sia adatta ai bambini e conforme a tutte le leggi vigenti.

Leggi informazioni sui requisiti del programma e delle Norme per le famiglie e consulta l'elenco di controllo interattivo sul portale Academy for App Success.

Norme per le famiglie di Google Play

L'uso della tecnologia come strumento per arricchire la vita delle famiglie continua a crescere e i genitori sono sempre alla ricerca di contenuti sicuri e di alta qualità da condividere con i propri figli. Le tue app possono essere progettate appositamente per bambini e ragazzi oppure potrebbero attirare semplicemente la loro attenzione. Google Play vuole aiutarti a garantire che siano sicure per tutti gli utenti, comprese le famiglie.

Il termine "bambino/ragazzo" può assumere significati diversi a seconda dei paesi e dei contesti. È importante che tu ti rivolga a un consulente legale che ti aiuti a determinare gli eventuali obblighi e/o le restrizioni in base alle fasce d'età applicabili alla tua app. Dato che tu sai meglio di chiunque come funziona la tua app, ci affidiamo a te per garantire che le app disponibili su Google Play siano sicure per le famiglie.

Per tutte le app conformi alle Norme per le famiglie di Google Play è possibile richiedere che vengano classificate per il programma App approvate dagli insegnanti, ma non possiamo garantire che

verranno incluse nel programma.

Requisiti di Play Console

Pubblico di destinazione e contenuti

Nella sezione Pubblico di destinazione e contenuti di Google Play Console, devi indicare il pubblico di destinazione della tua app, prima della pubblicazione, selezionandolo dall'elenco delle fasce d'età fornite. Indipendentemente dalla tua selezione in Google Play Console, qualora tu scelga di includere nella tua app immagini e termini che potrebbero essere considerati come destinati ai bambini, ciò potrà influire sulla valutazione di Google Play in merito al pubblico di destinazione dichiarato. Google Play si riserva il diritto di rivedere le informazioni sull'app fornite per determinare se il pubblico di destinazione indicato sia corretto.

Ti invitiamo a selezionare più fasce di età per il pubblico di destinazione della tua app soltanto se l'hai progettata, e sei certo che sia idonea, per gli utenti inclusi nelle fasce di età selezionate. Ad esempio, per le app progettate per i bambini di età compresa fra 1 e 5 anni e di età inferiore è necessario selezionare "Fino a 5 anni". Se l'app è progettata per uno specifico livello di istruzione, scegli la fascia d'età che lo definisce meglio. Seleziona le fasce d'età che includono sia adulti che bambini soltanto se l'app è stata pensata per utenti di tutte le età.

Aggiornamenti alla sezione Pubblico di destinazione e contenuti

Puoi sempre aggiornare le informazioni relative alla tua app nella sezione Pubblico di destinazione e contenuti di Google Play Console. È necessario un aggiornamento dell'app prima che tali informazioni siano riportate nel Google Play Store. Tuttavia, eventuali modifiche apportate in questa sezione di Google Play Console potranno essere esaminate per verificarne la conformità alle norme anche prima di inviare un aggiornamento dell'app.

Ti consigliamo vivamente di comunicare agli utenti eventuali modifiche della fascia d'età scelta come target per l'app o l'inserimento di annunci o acquisti in-app, utilizzando la sezione "Novità" della pagina relativa alla scheda dello Store dell'app o tramite notifiche in-app.

Rappresentazioni ingannevoli in Play Console

La rappresentazione ingannevole di qualsiasi informazione inerente la tua app in Play Console, inclusa la sezione Pubblico di destinazione e contenuti, potrebbe comportare la rimozione o la sospensione dell'app, perciò è importante fornire informazioni precise.

Requisiti delle Norme per le famiglie

Se il pubblico di destinazione della tua app include bambini e ragazzi, devi soddisfare i requisiti seguenti. Il mancato rispetto di questi requisiti può comportare la rimozione o la sospensione dell'app.

1. **Contenuti delle app:** i contenuti delle app accessibili a bambini e ragazzi devono essere adeguati per questi ultimi. Se include contenuti per utenti minorenni non ritenuti appropriati in tutto il mondo ma solo in una specifica regione, l'app potrebbe essere disponibile esclusivamente nella regione in questione (regioni con limitazioni).
2. **Funzionalità dell'app:** l'app non deve limitarsi a fornire una WebView di un sito web, né avere come finalità principale l'indirizzamento di traffico affiliato a un sito web senza l'autorizzazione del proprietario o dell'amministratore del sito web.
3. **Risposte di Play Console:** devi rispondere con precisione alle domande relative alla tua app contenute in Play Console e aggiornare queste risposte in base a qualsiasi modifica apportata all'app. Devi, ad esempio, dare risposte precise sulla tua app nella sezione Pubblico di destinazione e contenuti, nella sezione Sicurezza dei dati e nel questionario relativo alla classificazione dei contenuti dell'IARC.
4. **Pratiche relative ai dati:** devi comunicare la raccolta di eventuali informazioni personali e sensibili relative a bambini e ragazzi nell'app, compresa la raccolta tramite API e SDK richiamati o utilizzati nell'app. Le informazioni sensibili relative a bambini e ragazzi includono, a titolo esemplificativo, le

informazioni di autenticazione, i dati dei sensori della fotocamera e del microfono, i dati del dispositivo, l'ID Android e i dati sull'utilizzo degli annunci. Devi inoltre assicurarti che la tua app rispetti le seguenti pratiche relative ai dati:

- Le app destinate esclusivamente ai bambini e ragazzi non devono trasmettere identificatore pubblicità di Android (AAID), numero di serie della SIM, numero di serie nella build, BSSID, MAC, SSID, IMEI e/o IMSI.
  - Le app destinate esclusivamente ai bambini e ragazzi non devono richiedere l'autorizzazione AD_ID se hanno come target l'API Android 33 o versioni successive.
- Le app destinate sia a bambini e ragazzi sia a un pubblico più adulto non devono trasmettere AAID, numero di serie della SIM, numero di serie nella build, BSSID, MAC, SSID, IMEI e/o IMSI relativi a bambini e ragazzi o utenti di età sconosciuta.
- TelephonyManager dell'API Android non deve richiedere il numero di telefono del dispositivo.
- Le app rivolte esclusivamente a bambini e ragazzi non possono richiedere l'autorizzazione di accesso alla posizione oppure raccogliere, usare e trasmettere la posizione esatta.
- Le app devono utilizzare Companion Device Manager (CDM) quando richiedono l'utilizzo del Bluetooth, a meno che l'app non sia destinata solo a versioni di sistema operativo dei dispositivi non compatibili con CDM.

5. **API e SDK:** devi assicurarti che l'app implementi correttamente eventuali API e SDK.
   - Le app destinate esclusivamente ai bambini e ragazzi non devono contenere API o SDK non approvati per l'utilizzo in servizi rivolti principalmente ai minori.
     - Ad esempio, un servizio API che utilizza la tecnologia OAuth per l'autenticazione e l'autorizzazione, i cui termini di servizio non ne consentono l'utilizzo nei servizi rivolti a bambini e ragazzi.
   - Le app destinate sia a bambini e ragazzi sia a un pubblico più adulto non devono implementare API o SDK non approvati per l'utilizzo nei servizi rivolti ai minori, a meno che non vengano utilizzati dietro un filtro di controllo dell'età o implementati in un modo che non comporti la raccolta di dati di bambini e ragazzi. Le app destinate sia a bambini e ragazzi sia a un pubblico più adulto non devono richiedere agli utenti di eseguire l'accesso o accedere ai contenuti dell'app tramite un'API o un SDK non approvati per l'utilizzo nei servizi rivolti ai minori.

6. **Realtà aumentata (AR):** se l'app utilizza la realtà aumentata, devi includere un avviso di sicurezza che venga visualizzato subito dopo l'avvio della sezione AR. L'avviso dovrà contenere quanto segue:
   - Un messaggio appropriato relativo all'importanza della supervisione dei genitori.
   - Un promemoria che ricordi i rischi fisici nel mondo reale (ad esempio indicando all'utente di prestare attenzione a ciò che lo circonda).
   - L'app non deve richiedere l'utilizzo di dispositivi il cui uso è sconsigliato da parte di bambini e ragazzi (ad esempio Daydream, Oculus).

7. **Funzionalità e applicazioni social:** se l'app consente agli utenti di condividere o scambiare informazioni, devi comunicare con precisione queste funzionalità nel questionario relativo alla classificazione dei contenuti su Play Console.
   - App social: un'app social è un'app il cui scopo principale è consentire agli utenti di condividere contenuti in formato libero o di comunicare con ampi gruppi di persone. Per tutte le app social con un pubblico di destinazione che comprende bambini e ragazzi, prima di consentire a bambini e ragazzi di scambiare informazioni o contenuti multimediali in formato libero, è necessario fornire un promemoria in-app che ricordi la necessità di mantenere la sicurezza online e il rischio nel mondo reale che comporta l'interazione online. Devi inoltre richiedere l'intervento di un adulto prima di consentire a bambini e ragazzi di scambiare informazioni personali.
   - Funzionalità social: si intende per funzionalità social qualsiasi funzionalità aggiuntiva dell'app che consente agli utenti di condividere contenuti in formato libero o di comunicare con ampi gruppi di persone. Per tutte le app con un pubblico di destinazione che comprende bambini e ragazzi e che hanno funzionalità social, prima di consentire a bambini e ragazzi di scambiare informazioni o contenuti multimediali in formato libero, è necessario fornire un promemoria in-app che ricordi la

necessità di mantenere la sicurezza online e il rischio nel mondo reale che comporta l'interazione online. Devi inoltre fornire agli adulti un metodo per gestire le funzionalità social per bambini e ragazzi incluse, a titolo esemplificativo, l'attivazione/la disattivazione della funzionalità social o la selezione di diversi livelli di funzionalità. Infine devi richiedere l'intervento di una persona adulta prima di attivare funzionalità che consentano a bambini e ragazzi di scambiare informazioni personali.

- A questo scopo, devi avere un meccanismo per verificare che gli utenti non siano bambini o ragazzi senza incoraggiarli a falsificare la loro età per avere accesso ad aree della tua app rivolte agli adulti (ad esempio PIN, password, data di nascita, verifica email, documento di identità con fotografia, carta di credito o codice fiscale di una persona adulta).
- Le app social il cui scopo principale è consentire di chattare con sconosciuti non devono essere rivolte a bambini e ragazzi. Alcuni esempi sono: app in stile chat roulette, app di incontri, chat room aperte rivolte a bambini e ragazzi e così via.

8. **Conformità legale:** devi assicurarti che l'app, compresi eventuali API o SDK chiamati o utilizzati dall'app stessa, sia conforme alla legge statunitense Children's Online Privacy Protection Act (COPPA) , al Regolamento generale sulla protezione dei dati (GDPR) dell'UE e a eventuali altre leggi o normative vigenti.

Di seguito sono riportati alcuni esempi di violazioni frequenti:

- App che promuovono giochi per bambini nella scheda dello Store, ma il cui contenuto è appropriato solo per un pubblico adulto.
- App che implementano API i cui termini di servizio ne vietano l'utilizzo in app rivolte ai minori.
- App che promuovono un'immagine positiva dell'uso di alcol, tabacco o sostanze controllate.
- App che includono giochi e scommesse reali o simulati.
- App con violenza, spargimenti di sangue e contenuti scioccanti non adatti a bambini e ragazzi.
- App che offrono servizi di incontri oppure consulenza sessuale o matrimoniale.
- App che contengono link a siti web che presentano contenuti che violano le Norme del programma per gli sviluppatori di Google Play.
- App che mostrano a bambini e ragazzi annunci destinati a un pubblico adulto (ad esempio, contenuti violenti, di natura sessuale o collegati a giochi e scommesse).

Annunci e monetizzazione

Se monetizzi un'app rivolta a bambini e ragazzi su Google Play, è importante che l'app sia conforme ai requisiti delle norme che seguono relative agli annunci e alla monetizzazione per le famiglie.

Le norme riportate di seguito si applicano alla monetizzazione e alla pubblicità nell'app, inclusi annunci, promozioni incrociate (per le app tue e di terze parti), offerte relative ad acquisti in-app o qualsiasi altro contenuto commerciale (come il posizionamento di prodotti a pagamento). La monetizzazione e la pubblicità in queste app devono essere conformi a tutte le leggi e normative vigenti (incluse eventuali indicazioni di settore o di autoregolamentazione pertinenti).

Google Play si riserva il diritto di rifiutare, rimuovere o sospendere le app in caso di tattiche commerciali eccessivamente aggressive.

Requisiti degli annunci

Se la tua app visualizza annunci per bambini e ragazzi o utenti di età sconosciuta, devi:

- usare soltanto SDK per gli annunci autocertificati per la famiglia di Google Play per mostrare annunci a questi utenti;
- garantire che gli annunci mostrati a questi utenti non prevedano pubblicità basata sugli interessi (pubblicità indirizzata a singoli utenti che hanno determinate caratteristiche sulla base del loro comportamento di navigazione online) o remarketing (pubblicità indirizzata a singoli utenti sulla base di interazioni precedenti con un'app o un sito web);

- garantire che gli annunci mostrati a questi utenti presentino contenuti appropriati per bambini e ragazzi;
- garantire che gli annunci mostrati a questi utenti rispettino i requisiti relativi al formato degli annunci per le famiglie; e
- garantire la conformità a tutte le normative legali vigenti e a tutti gli standard di settore applicabili in materia di pubblicità destinata a bambini e ragazzi.

Requisiti per i formati degli annunci

La monetizzazione e la pubblicità nell'app non devono avere contenuti ingannevoli o essere strutturate in modo da determinare clic involontari da parte di utenti minorenni.

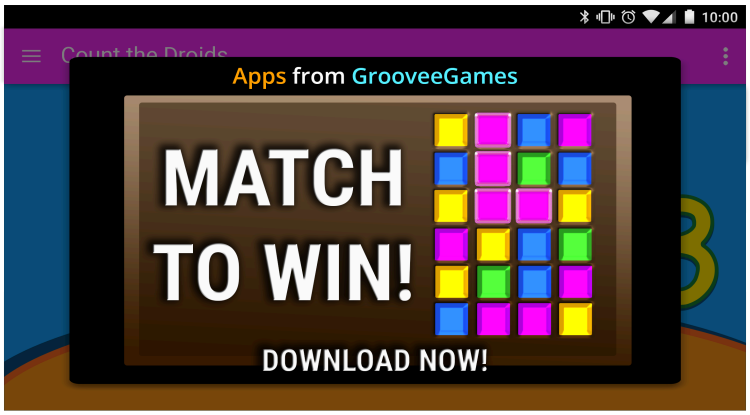
Se il pubblico di destinazione della tua app è costituito soltanto da bambini e ragazzi, è vietato quanto indicato di seguito. Se il pubblico di destinazione della tua app è costituito da bambini e ragazzi e da un pubblico più adulto, è vietato quanto segue in caso di pubblicazione di annunci per bambini e ragazzi o utenti di età sconosciuta:

- Contenuti di monetizzazione e pubblicità che generano interruzioni dell'esperienza utente, inclusi quelli che occupano l'intero schermo o che interferiscono con il normale utilizzo senza fornire un modo chiaro per chiudere l'annuncio (ad esempio ad wall).
- Contenuti di monetizzazione e pubblicità che interferiscono con il normale gameplay o utilizzo dell'app, inclusi annunci con premio o di attivazione, e che non possono essere chiusi dopo 5 secondi.
- Contenuti di monetizzazione e pubblicità che non interferiscono con il normale gameplay o utilizzo dell'app possono rimanere visualizzati per più di 5 secondi (ad esempio, contenuti video con annunci integrati).
- Contenuti di monetizzazione e pubblicità interstitial visualizzati contestualmente all'avvio dell'app.
- Più posizionamenti dell'annuncio in una pagina (ad esempio, sono vietati annunci banner che mostrano più offerte nello stesso posizionamento, così come la visualizzazione di più annunci banner o video).
- Contenuti di monetizzazione e pubblicità che non sono chiaramente distinguibili dai contenuti dell'app, ad esempio Offerwall e altre esperienze pubblicitarie immersive.
- Uso di tattiche emotivamente manipolative o scioccanti per incoraggiare la visualizzazione di annunci o gli acquisti in-app.
- Annunci ingannevoli che obbligano l'utente a eseguire il clickthrough usando un pulsante di chiusura per attivare un altro annuncio o facendo apparire improvvisamente gli annunci in aree dell'app che generalmente l'utente tocca per accedere a un'altra funzione.
- Mancata distinzione tra l'uso di monete virtuali nei giochi rispetto a soldi reali per effettuare acquisti in-app.

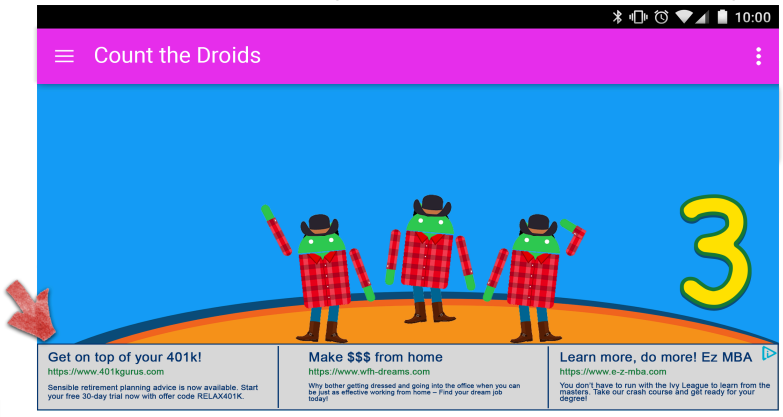
Di seguito sono riportati alcuni esempi di violazioni frequenti:

- Monetizzazione e pubblicità che si allontanano dal dito dell'utente mentre questi tenta di chiuderle.
- Monetizzazione e pubblicità che non forniscono all'utente un modo per chiudere l'offerta dopo cinque (5) secondi, come illustrato nell'esempio seguente:

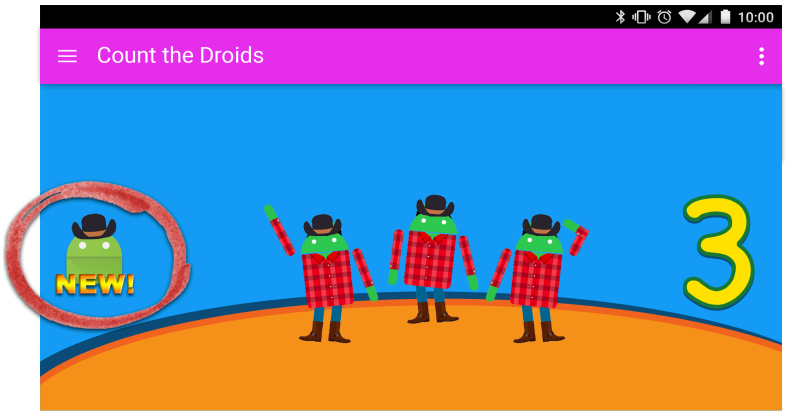
- Monetizzazione e pubblicità che occupano quasi tutto lo schermo del dispositivo senza fornire all'utente un modo chiaro per chiuderle, come illustrato nell'esempio seguente:



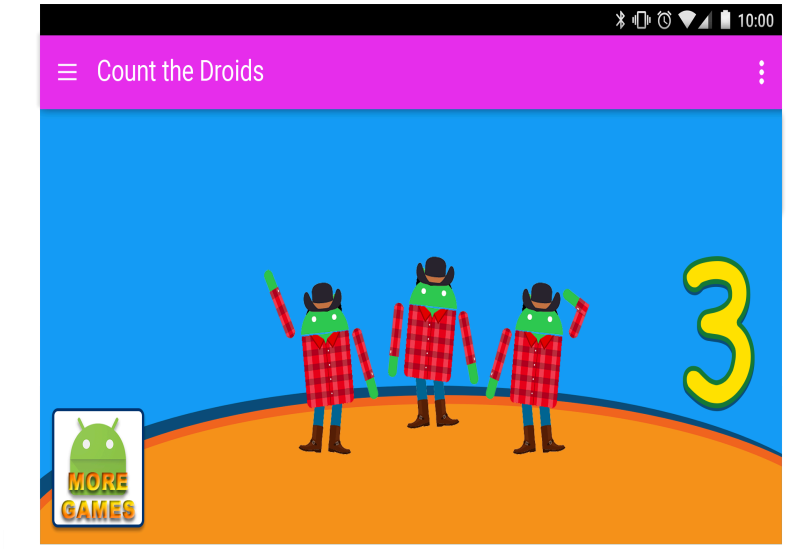
- Annunci banner che mostrano più offerte, come illustrato nell'esempio seguente:



- Monetizzazione e pubblicità che l'utente potrebbe scambiare per contenuti dell'app, come illustrato nell'esempio seguente:



- Pulsanti, annunci o altra monetizzazione che promuovono le altre tue schede dello Store in Google Play, ma che non sono distinguibili dai contenuti dell'app, come illustrato nell'esempio seguente:



Di seguito sono riportati alcuni esempi di contenuti di annunci inappropriati che non dovrebbero essere mostrati a bambini e ragazzi.

- **Contenuti multimediali inappropriati**: annunci relativi a programmi TV, film, album musicali o altri contenuti non adatti a bambini e ragazzi.
- **Videogiochi e software scaricabile inappropriati**: annunci relativi a software scaricabile e videogiochi non adatti a bambini e ragazzi.
- **Sostanze controllate o nocive**: annunci relativi ad alcol, tabacco, sostanze controllate o altre sostanze nocive.
- **Giochi e scommesse**: annunci relativi a simulazioni di giochi e scommesse, promozioni di concorsi o lotterie, anche se la partecipazione non prevede costi.
- **Contenuti per adulti e a sfondo sessuale**: annunci con contenuti sessuali, sessualmente allusivi e inappropriati per i minori.
- **Incontri o relazioni**: annunci relativi a siti di incontri o relazioni per adulti.
- **Contenuti violenti**: annunci con contenuti violenti ed espliciti non adatti a bambini e ragazzi.

SDK per gli annunci

Se pubblichi annunci nella tua app e il relativo pubblico di destinazione è costituito esclusivamente da bambini e ragazzi, devi utilizzare soltanto versioni dell'SDK per gli annunci autocertificati per la famiglia . Se il pubblico di destinazione dell'app è costituito sia da bambini e ragazzi sia da utenti più adulti, devi implementare misure di controllo dell'età, come un filtro di controllo dell'età , e

assicurarti che gli annunci mostrati a bambini e ragazzi provengano esclusivamente da versioni dell'SDK per gli annunci autocertificati di Google Play.

Visita la pagina delle norme del Programma relativo all'SDK per gli annunci autocertificati per la famiglia per avere maggiori informazioni su questi requisiti e questa pagina per vedere l'attuale elenco di versioni dell'SDK per gli annunci autocertificati per la famiglia.

Se utilizzi AdMob, consulta il Centro assistenza AdMob per ulteriori informazioni sui prodotti.

È tua responsabilità garantire che l'app soddisfi tutti i requisiti relativi a pubblicità, acquisti in-app e contenuti commerciali. Contatta il/i provider di SDK per gli annunci per avere ulteriori informazioni sulle rispettive norme relative ai contenuti e prassi pubblicitarie.

Norme relative all'SDK per gli annunci autocertificati per la famiglia

Google Play si impegna a creare un'esperienza sicura per bambini e ragazzi e famiglie. Una parte fondamentale di questo impegno è garantire che bambini e ragazzi vedano soltanto annunci adatti alla loro età e che i loro dati vengano gestiti in modo appropriato. Per raggiungere questo obiettivo richiediamo per SDK per gli annunci e piattaforme di mediazione un'autocertificazione che attesti che sono adatti a bambini e ragazzi e conformi alle Norme del programma per gli sviluppatori di Google Play e alle Norme per le famiglie di Google Play, inclusi i requisiti del Programma relativo all'SDK per gli annunci autocertificati per la famiglia.

Il Programma relativo all'SDK per gli annunci autocertificati per la famiglia di Google Play è importante per gli sviluppatori perché consente loro di identificare gli SDK per gli annunci o le piattaforme di mediazione che dispongono dell'autocertificazione che attesta che sono adatti per essere utilizzati in app progettate specificamente per bambini e ragazzi.

La rappresentazione ingannevole di qualsiasi informazione inerente l'SDK, anche nella domanda presentata tramite il modulo di interesse, potrebbe comportare la rimozione o la sospensione dell'SDK dal Programma relativo all'SDK per gli annunci autocertificati per la famiglia, pertanto è importante fornire informazioni precise.

Requisiti previsti dalle norme

Se il tuo SDK o la tua piattaforma di mediazione gestisce app che fanno parte del programma Per la famiglia di Google Play, devi rispettare tutte le norme per gli sviluppatori di Google Play, inclusi i requisiti che seguono. Il mancato rispetto di uno o più requisiti previsti dalle norme potrebbe comportare la rimozione o la sospensione dal Programma relativo all'SDK per gli annunci autocertificati per la famiglia.

È tua responsabilità garantire la conformità del tuo SDK o della tua piattaforma di mediazione; assicurati di leggere le Norme del programma per gli sviluppatori di Google Play, le Norme per le famiglie di Google Play e i requisiti del Programma relativo all'SDK per gli annunci autocertificati per la famiglia.

1. **Contenuti degli annunci:** i contenuti degli annunci accessibili a bambini e ragazzi devono essere adeguati per questi ultimi.
   - Devi (i) definire i contenuti degli annunci e i comportamenti discutibili e (ii) vietarli nei tuoi termini o nelle tue norme. Le definizioni devono essere conformi alle Norme del programma per gli sviluppatori di Google Play.
   - Devi inoltre creare un metodo per classificare le creatività degli annunci in base alle fasce d'età appropriate. Queste ultime devono includere almeno le fasce Per tutti e Per adulti. La metodologia di classificazione deve essere in linea con la metodologia che Google fornisce agli SDK una volta che è stato compilato il modulo di interesse.
   - Devi assicurarti che, quando le offerte in tempo reale vengono utilizzate per mostrare annunci a bambini e ragazzi, le creatività siano state esaminate e siano conformi ai requisiti indicati in precedenza.

- Devi anche avere un meccanismo per identificare visivamente le creatività provenienti dal tuo inventario (ad esempio l'aggiunta di una filigrana alla creatività dell'annuncio, che può essere un logo visivo della tua società o una funzionalità simile).

2. **Formato degli annunci:** devi assicurarti che tutti gli annunci mostrati a utenti minorenni rispettino i requisiti per i formati degli annunci per le famiglie e devi consentire agli sviluppatori di selezionare formati degli annunci conformi alle Norme per le famiglie di Google Play.
   - La pubblicità non deve avere contenuti ingannevoli o essere strutturata in modo da determinare clic involontari da parte di utenti minorenni. Non sono consentiti annunci ingannevoli che obbligano l'utente a eseguire il clickthrough usando un pulsante di chiusura per attivare un altro annuncio o facendo apparire improvvisamente gli annunci in aree dell'app che generalmente l'utente tocca per accedere a un'altra funzione.
   - La pubblicità improvvisa, inclusa la pubblicità che occupa l'intero schermo o che interferisce con il normale utilizzo e non fornisce un modo chiaro per ignorare l'annuncio (ad esempio ad wall), non è consentita.
   - La pubblicità che interferisce con il normale gameplay o utilizzo dell'app, inclusi annunci con premio, deve poter essere chiusa dopo 5 secondi.
   - Non sono consentiti posizionamenti di più annunci nella stessa pagina. Ad esempio, sono vietati annunci banner che mostrano più offerte nello stesso posizionamento, così come la visualizzazione di più annunci banner o video).
   - La pubblicità deve essere chiaramente distinguibile dai contenuti dell'app. Non sono consentite Offerwall ed esperienze pubblicitarie immersive che non sono chiaramente identificabili come pubblicità dagli utenti minorenni.
   - La pubblicità non deve usare tattiche emotivamente manipolative o scioccanti per incoraggiare la visualizzazione di annunci.
3. **IBA (pubblicità basata sugli interessi)/remarketing:** devi assicurarti che gli annunci mostrati a utenti minorenni non prevedano pubblicità basata sugli interessi (pubblicità indirizzata a singoli utenti che hanno determinate caratteristiche sulla base del loro comportamento di navigazione online) o remarketing (pubblicità indirizzata a singoli utenti sulla base di interazioni precedenti con un'app o un sito web).
4. **Pratiche relative ai dati:** in qualità di provider di SDK, devi assicurare la trasparenza in merito alla modalità di gestione dei dati utente (ad esempio le informazioni fornite da un utente o raccolte in relazione a un utente, incluse le informazioni del dispositivo). Ciò significa comunicare l'accesso, la raccolta, l'uso e la condivisione dei dati da parte dell'SDK e limitare l'uso dei dati alle finalità comunicate. I presenti requisiti di Google Play si aggiungono ai requisiti previsti dalle leggi vigenti in materia di privacy e protezione dei dati. Devi comunicare la raccolta di eventuali informazioni personali e sensibili relative a bambini e ragazzi incluse, a titolo esemplificativo, le informazioni di autenticazione, i dati dei sensori della fotocamera e del microfono, i dati del dispositivo, l'ID Android e i dati sull'utilizzo degli annunci.
   - Devi consentire agli sviluppatori, in base alle singole richieste o in relazione a singole app, di richiedere il trattamento per siti o servizi destinati ai minori per la pubblicazione di annunci. Questo trattamento deve essere conforme alle leggi e normative vigenti, come la legge statunitense Children's Online Privacy Protection Act (COPPA) e il Regolamento generale sulla protezione dei dati (GDPR) dell'UE .
     - Google Play richiede che gli SDK per gli annunci disattivino annunci personalizzati, pubblicità basata sugli interessi e remarketing nell'ambito del trattamento per siti o servizi destinati ai minori.
   - Devi assicurarti che, quando le offerte in tempo reale vengono utilizzate per mostrare annunci a bambini e ragazzi, gli indicatori relativi alla privacy vengano applicati agli offerenti.
   - Non devi trasmettere AAID, numero di serie della SIM, numero di serie nella build, BSSID, MAC, SSID, IMEI e/o IMSI relativi a bambini e ragazzi o utenti di età sconosciuta.
5. **Piattaforme di mediazione:** quando mostri annunci a bambini e ragazzi devi fare quanto segue.

- Utilizza solo SDK per gli annunci autocertificati per la famiglia o implementa le salvaguardie necessarie per garantire che tutti gli annunci pubblicati dalle reti di mediazione siano conformi a questi requisiti.
- Trasmetti le informazioni necessarie alle piattaforme di mediazione per indicare la classificazione dei contenuti degli annunci e l'eventuale trattamento applicabile per siti o servizi destinati ai minori.

6. **Autocertificazione e conformità:** devi fornire a Google informazioni sufficienti, ad esempio le informazioni indicate nel modulo di interesse , per verificare la conformità dell'SDK per gli annunci a tutti i requisiti di autocertificazione, inclusi, a titolo esemplificativo:
   - Fornire una versione in lingua inglese dei Termini di servizio, delle norme sulla privacy e della Guida all'integrazione per i publisher del tuo SDK o della tua piattaforma di mediazione.
   - Inviare un'app di prova di esempio che usi l'ultima versione conforme dell'SDK per gli annunci. L'app di prova di esempio deve essere un APK Android completo ed eseguibile che utilizza tutte le funzionalità dell'SDK. Requisiti dell'app di prova:
     - Deve essere inviata sotto forma di APK Android completo ed eseguibile, pensato per essere eseguito sul fattore di forma di uno smartphone.
     - Deve utilizzare l'ultima versione rilasciata dell'SDK per gli annunci o una versione che sta per essere rilasciata che sia conforme alle norme di Google Play.
     - Deve utilizzare tutte le funzionalità dell'SDK per gli annunci, inclusa la chiamata all'SDK per recuperare e visualizzare gli annunci.
     - Deve avere accesso completo a tutti gli inventari pubblicitari attualmente pubblicati o che saranno pubblicati in futuro sulla rete tramite le creatività richieste con l'app di prova.
     - Non deve essere limitata dalla geolocalizzazione.
     - Se l'inventario è per un pubblico misto, l'app di prova deve essere in grado di distinguere tra le richieste di creatività degli annunci dall'inventario completo e dall'inventario adatto ai bambini o a tutte le fasce d'età.
     - Non deve essere limitata ad annunci specifici all'interno dell'inventario, a meno che non sia controllata dal filtro di controllo dell'età.

7. Devi rispondere tempestivamente a eventuali richieste successive di informazioni e autocertificare che tutte le nuove versioni siano conformi alle Norme del programma per gli sviluppatori di Google Play più recenti, inclusi i requisiti delle Norme per le famiglie.
8. **Conformità legale:** gli SDK per gli annunci autocertificati per la famiglia devono supportare la pubblicazione di annunci in conformità con tutte le leggi e normative vigenti relative a bambini e ragazzi che possano applicarsi ai rispettivi publisher.
   - Devi assicurarti che l'SDK o la piattaforma di mediazione sia conforme alla legge statunitense Children's Online Privacy Protection Act (COPPA) , al Regolamento generale sulla protezione dei dati (GDPR) dell'UE e a qualsiasi altra legge o normativa vigente.

     Nota: il termine "bambini e ragazzi" può assumere significati diversi a seconda dei paesi e dei contesti. È importante che tu ti rivolga a un consulente legale che ti aiuti a stabilire le eventuali obbligazioni e/o restrizioni in base alle fasce d'età applicabili alla tua app. Dato che tu sai meglio di chiunque altro come funziona la tua app, ci affidiamo a te per garantire che le app disponibili su Google Play siano sicure per le famiglie.

Visita la pagina Programma relativo all'SDK per gli annunci autocertificati per la famiglia per avere maggiori informazioni sui requisiti del programma.

Applicazione

Evitare le violazioni delle norme è sempre meglio che doverle gestire ma, qualora si verifichino, ci impegniamo ad assicurare che gli sviluppatori sappiano come rendere conformi le loro app. Ti

invitiamo a comunicarci eventuali violazioni riscontrate o a porci eventuali domande sulla gestione delle violazioni .

Copertura delle norme

Le nostre norme si applicano a qualsiasi contenuto mostrato o reso disponibile dall'app tramite link, compresi eventuali annunci mostrati agli utenti ed eventuali contenuti generati dagli utenti che siano ospitati o resi disponibili dall'app tramite link. Si applicano, inoltre, a qualsiasi contenuto del tuo account sviluppatore mostrato pubblicamente su Google Play, inclusi il tuo nome sviluppatore e la pagina di destinazione del tuo sito web dello sviluppatore specificato.

Sono vietate le app che consentono agli utenti di installare altre app sui propri dispositivi. Le app che forniscono accesso ad altre app, giochi o software senza installazione, incluse le funzionalità e le esperienze offerte da terze parti, devono garantire che tutti i contenuti a cui forniscono l'accesso ottemperino a tutte le norme di Google Play e che possano anche essere soggette a ulteriori revisioni secondo le norme.

I termini definiti utilizzati in queste norme hanno lo stesso significato che hanno nel Contratto di distribuzione per gli sviluppatori (DDA, attribuzione basata sui dati). Oltre a rispettare queste norme e il Contratto di distribuzione per gli sviluppatori, i contenuti dell'app devono essere classificati in conformità con le nostre Linee guida per la classificazione dei contenuti.

Sono vietati le app o i contenuti di app che compromettono la fiducia degli utenti nell'ecosistema di Google Play. Nel valutare se includere o rimuovere un'app da Google Play, prendiamo in considerazione una serie di fattori inclusi, a titolo esemplificativo, un comportamento dannoso ricorrente o un rischio elevato di comportamento illecito. Identifichiamo il rischio di comportamento illecito in base a elementi quali, a titolo esemplificativo, reclami relativi ad app e sviluppatori specifici, segnalazioni di notizie, cronologia delle violazioni precedenti, feedback degli utenti, uso di brand e personaggi noti e altre risorse.

Funzionamento di Google Play Protect

Google Play Protect controlla le app quando le installi. Inoltre esegue periodicamente la scansione del dispositivo. Se rileva un'app potenzialmente dannosa, potrebbe:

- Inviare una notifica. Per rimuovere l'app, tocca la notifica, quindi tocca Disinstalla.
- Disattivare l'app fino a quando non viene disinstallata.
- Rimuovere automaticamente l'app: nella maggior parte dei casi, quando viene rilevata un'app dannosa, ricevi una notifica che comunica che l'app è stata rimossa.

Funzionamento della protezione antimalware

Per proteggerti da URL e software dannosi di terze parti e da altri problemi di sicurezza, Google potrebbe ricevere informazioni su:

- Connessioni di rete del dispositivo
- URL potenzialmente dannosi
- Sistema operativo e app installate sul dispositivo tramite Google Play o altre origini

Potresti ricevere un avviso da Google che segnala un'app o un URL potenzialmente non sicuri. Google potrebbe rimuovere l'URL o l'app oppure bloccarne l'installazione, qualora sia noto che l'app o l'URL sono dannosi per dispositivi, dati o utenti.

Puoi scegliere di disattivare alcune di queste protezioni nelle impostazioni del dispositivo. Tuttavia Google potrebbe continuare a ricevere informazioni sulle app installate tramite Google Play e le app installate sul dispositivo da altre fonti potrebbero continuare a essere controllate per individuare problemi di sicurezza, senza l'invio di informazioni a Google.

Funzionamento degli avvisi sulla privacy

Google Play Protect avvisa se un'app viene rimossa dal Google Play Store perché potrebbe accedere alle informazioni personali; sarà possibile disinstallare l'app.

Procedura di applicazione

Durante l'esame di contenuti o account per stabilire se sono illegali o violano le nostre norme, prendiamo in considerazione varie informazioni per prendere una decisione, come metadati dell'app (ad esempio titolo e descrizione), esperienza nell'app, dati dell'account (ad esempio precedenti violazioni delle norme) e altre informazioni fornite tramite meccanismi di segnalazione (ove pertinente) e controlli fatti di propria iniziativa.

Se la tua app o il tuo account sviluppatore viola una delle nostre norme, adotteremo gli opportuni provvedimenti, come descritto di seguito. Inoltre, ti forniremo via email informazioni pertinenti sul provvedimento che abbiamo adottato, insieme alle istruzioni su come presentare ricorso se ritieni che ci sia stato un errore.

Tieni presente che le comunicazioni amministrative o relative a rimozioni potrebbero non indicare ogni singola violazione delle norme riscontrata nel tuo account, nella tua app o nel più ampio catalogo di app. È responsabilità degli sviluppatori risolvere eventuali problemi relativi alle norme e verificare con la dovuta attenzione che le altre parti dell'app o dell'account siano completamente conformi alle norme. La mancata risoluzione delle violazioni delle norme nel tuo account e in tutte le tue app potrebbe comportare ulteriori provvedimenti.

Violazioni gravi o ripetute (quali malware, attività fraudolente e app che potrebbero arrecare danno all'utente o al dispositivo) di queste norme o del Contratto di distribuzione per gli sviluppatori (DDA) comporteranno la chiusura di account sviluppatore Google Play singoli o correlati.

Provvedimenti

I diversi provvedimenti possono influire sulle tue app in modi diversi. Utilizziamo una combinazione di valutazioni automatiche e manuali per esaminare le app e i relativi contenuti al fine di individuare e valutare i contenuti che violano le nostre norme e sono dannosi per gli utenti e per l'ecosistema di Google Play in generale. L'uso di modelli automatici ci consente di rilevare più violazioni e di valutare più velocemente potenziali problemi, aiutandoci a mantenere Google Play sicuro per tutti. I contenuti che violano le norme vengono rimossi dai nostri modelli automatici oppure, se è necessario un accertamento più preciso, vengono contrassegnati per essere esaminati ulteriormente da operatori e analisti qualificati che effettuano le valutazioni dei contenuti, ad esempio se è necessario capirne il contesto. I risultati di queste revisioni manuali vengono poi utilizzati per creare dati di addestramento che ci aiutano a migliorare ulteriormente i nostri modelli di machine learning.

Nella sezione che segue vengono descritti i vari provvedimenti che Google Play potrebbe adottare e il relativo impatto sulla tua app e/o sul tuo account sviluppatore Google Play.

Se non indicato diversamente in una comunicazione relativa all'applicazione, questi provvedimenti sono validi per tutte le regioni. Ad esempio, se la tua app viene sospesa, non sarà disponibile in tutte le regioni. Inoltre, se non diversamente indicato, questi provvedimenti rimarranno in vigore, a meno che non presenti un ricorso contro un provvedimento che viene approvato.

Rifiuto

- Su Google Play non verranno resi disponibili le nuove app o gli aggiornamenti dell'app inviati per la revisione.
- Se un aggiornamento di un'app esistente viene rifiutato, la versione dell'app pubblicata prima di tale aggiornamento rimane disponibile su Google Play.
- I rifiuti non influiscono sul tuo accesso alle installazioni, alle statistiche e alle valutazioni esistenti degli utenti relative all'app rifiutata.

- I rifiuti non influiscono sulla reputazione del tuo account sviluppatore Google Play.

Ti ricordiamo di non inviare nuovamente un'app rifiutata prima di aver risolto tutte le violazioni delle norme.

Rimozione

- L'app e le eventuali versioni precedenti vengono rimosse da Google Play e non saranno più disponibili per il download.
- Poiché l'app viene rimossa, gli utenti non potranno vedere la relativa scheda dello Store. Queste informazioni verranno ripristinate una volta che avrai inviato un aggiornamento conforme alle norme per l'app rimossa.
- Gli utenti potrebbero non essere in grado di effettuare acquisti in-app o utilizzare funzionalità di fatturazione in-app finché una versione conforme alle norme non verrà approvata da Google Play.
- Le rimozioni non influiscono immediatamente sulla situazione di regolarità del tuo account sviluppatore Google Play, ma rimozioni multiple potrebbero comportare la sospensione dell'account.

Nota: non tentare di ripubblicare un'app rimossa finché non avrai risolto tutte le violazioni delle norme.

Sospensione

- L'app e le eventuali versioni precedenti vengono rimosse da Google Play e non saranno più disponibili per il download.
- La sospensione può verificarsi a causa di violazioni delle norme gravi o ripetute, nonché di rimozioni o rifiuti ripetuti di app.
- Poiché l'app viene sospesa, gli utenti non potranno vedere la relativa scheda dello Store.
- Non potrai più utilizzare l'APK o l'app bundle di un'app sospesa.
- Gli utenti non saranno in grado di effettuare acquisti in-app o utilizzare funzionalità di Fatturazione in-app.
- Le sospensioni incidono, in qualità di avvertimenti, sulla situazione di regolarità del tuo account sviluppatore Google Play. Più avvertimenti possono comportare la chiusura degli account sviluppatore Google Play individuali e correlati.

Visibilità limitata

- La rilevabilità dell'app su Google Play è limitata. L'app rimarrà disponibile su Google Play e sarà accessibile agli utenti con un link diretto alla scheda dello Store dell'app.
- Lo stato di Visibilità limitata dell'app non influisce sulla situazione di regolarità del tuo account sviluppatore Google Play.
- Lo stato di Visibilità limitata non incide sulla capacità degli utenti di vedere la scheda dello Store esistente dell'app.

Aree geografiche con limitazioni

- Gli utenti possono scaricare la tua app tramite Google Play soltanto in alcune aree geografiche.
- Gli utenti di altre aree geografiche non potranno trovare l'app sul Play Store.
- Gli utenti che avevano già installato l'app possono continuare a usarla sul proprio dispositivo, ma non riceveranno più aggiornamenti.
- La limitazione delle aree geografiche non influisce sullo stato di conformità del tuo account sviluppatore Google Play.

Stato limitato dell'account

- Quando il tuo account sviluppatore è in uno stato limitato, tutte le app nel tuo catalogo vengono rimosse da Google Play e non potrai più pubblicare nuove app o ripubblicare app esistenti. Continuerai ad avere accesso a Play Console.

- Poiché vengono rimosse tutte le app, gli utenti non potranno vedere la relativa scheda dello Store e il tuo profilo sviluppatore.
- Gli utenti attuali non saranno in grado di effettuare acquisti in-app o utilizzare funzionalità di fatturazione in-app delle tue app.
- Puoi continuare a usare Play Console per fornire ulteriori informazioni a Google Play e modificare i dati dell'account.
- Potrai ripubblicare le tue app dopo aver risolto tutte le violazioni delle norme.

Chiusura dell'account

- Quando il tuo account sviluppatore viene chiuso, tutte le app nel tuo catalogo verranno rimosse da Google Play e non potrai più pubblicare nuove app. Ciò significa anche che qualsiasi account sviluppatore Google Play correlato verrà sospeso definitivamente.
- Sospensioni ripetute o relative a violazioni gravi delle norme potrebbero comportare anche la chiusura del tuo account Play Console.
- Poiché le app all'interno dell'account chiuso vengono rimosse, gli utenti non potranno vedere la scheda dello Store dell'app e il tuo profilo sviluppatore.
- Gli utenti attuali non saranno in grado di effettuare acquisti in-app o utilizzare funzionalità di fatturazione in-app delle tue app.

Nota: anche tutti i nuovi account che tenterai di aprire verranno chiusi (senza rimborso della quota di registrazione sviluppatore). Quindi, se sei titolare di un account chiuso, non tentare di registrare un nuovo account Play Console.

Account inattivi

Gli account inattivi sono account sviluppatore non più attivi o abbandonati. Gli account inattivi non sono in regola come previsto dal Contratto di distribuzione per gli sviluppatori .

Gli account sviluppatore Google Play sono destinati a sviluppatori attivi che pubblicano e gestiscono attivamente le app. Per prevenire abusi, chiudiamo gli account inattivi o inutilizzati oppure non utilizzati in modo significativo (ad esempio per pubblicare e aggiornare app, accedere alle statistiche o gestire le schede dello Store) su base regolare.

La chiusura di un account inattivo eliminerà l'account ed eventuali dati associati. La tariffa di registrazione non è rimborsabile e verrà persa. Prima di chiudere l'account inattivo, invieremo una notifica all'utente tramite le relative informazioni di contatto fornite.

La chiusura di un account inattivo non limiterà la possibilità di creare un nuovo account in futuro qualora si decidesse di pubblicare su Google Play. L'account non potrà più essere riattivato e precedenti dati o app non saranno disponibili sul nuovo account.

Gestione e segnalazione di violazioni delle norme

Ricorso contro un provvedimento di applicazione

Reintegreremo l'applicazione se è stato commesso un errore ed emerge che l'applicazione non viola le norme del programma di Google Play e il Contratto di distribuzione per gli sviluppatori. Se, dopo aver esaminato attentamente le norme, ritieni che la nostra decisione possa essere erronea, segui le istruzioni fornite nella notifica via email relativa all'applicazione oppure fai clic qui per presentare ricorso.

Altre risorse

Per ulteriori informazioni riguardanti un provvedimento di applicazione o una valutazione/un commento di un utente, puoi consultare alcune delle risorse riportate di seguito o contattarci tramite il Centro

assistenza Google Play. Non siamo, tuttavia, in grado di fornire consulenza legale, per la quale dovrai rivolgerti a un consulente legale di fiducia.

- Verifica app
- Segnalare una violazione delle norme
- Contattare Google Play in merito alla chiusura dell'account o alla rimozione di app
- Avvisi imparziali
- Segnalare app e commenti inappropriati
- La mia app è stata rimossa da Google Play
- Informazioni sulla chiusura degli account sviluppatore Google Play

---

Requisiti di Play Console

Per garantire la sicurezza e la protezione del nostro vivace ecosistema di app, Google Play richiede a tutti gli sviluppatori di completare i requisiti di Play Console, inclusi eventuali profili collegati al rispettivo account sviluppatore Play Console. Le informazioni verificate verranno visualizzate su Google Play per contribuire a consolidare la fiducia degli utenti nei confronti degli sviluppatori. Scopri di più sulle informazioni mostrate su Google Play.

Google Play offre due tipi di account sviluppatore: Personale e Organizzazione. La scelta del tipo di account sviluppatore corretto e il completamento delle verifiche necessarie sono fondamentali per un'esperienza di onboarding fluida. Scopri di più sulla scelta del tipo di account sviluppatore.

Durante la creazione del tuo account Play Console, gli sviluppatori che forniscono i seguenti servizi devono registrarsi come organizzazione:

- Servizi e prodotti finanziari, inclusi, a titolo esemplificativo, servizi bancari, prestiti, compravendita di azioni, fondi di investimento, portafogli software di criptovalute e scambi di criptovalute. Scopri di più sulle norme relative ai servizi finanziari.
- App per la salute, come app mediche e app di ricerche su soggetti umani. Scopri di più sulle categorie di app per la salute.
- App approvate per l'utilizzo della classe VpnService . Scopri di più sulle norme relative al servizio VPN.
- App governative, incluse app sviluppate da o per conto di un ente statale.

Una volta selezionato un tipo di account, devi:

- Fornire in modo accurato i dati del tuo account sviluppatore, inclusi:
  - Nome legale e indirizzo
  - Numero DUNS , se ti registri come organizzazione
  - Indirizzo email di contatto e numero di telefono
  - Indirizzo email e numero di telefono dello sviluppatore indicati su Google Play (ove applicabili)
  - Metodi di pagamento (ove applicabili)
  - Profilo pagamenti Google collegato al tuo account sviluppatore
- Se ti registri come organizzazione, assicurati che i dati dell'account sviluppatore siano aggiornati e coerenti con tutti i dettagli archiviati nel tuo profilo di Dun & Bradstreet

Prima di inviare l'app, devi:

- Fornire in modo accurato tutte le informazioni e i metadati dell'app
- Caricare le norme sulla privacy dell'app e compilare i requisiti per la sezione Sicurezza dei dati
- Fornire un account demo attivo, informazioni di accesso e tutte le altre risorse necessarie a Google Play per la revisione della tua app (in particolare, credenziali di accesso, codice QR e così via)

Come sempre, dovresti assicurarti che la tua app fornisca un'esperienza utente stabile, coinvolgente e reattiva; verifica che tutti gli elementi della tua app, come reti pubblicitarie, servizi di analisi ed SDK di

terze parti, siano conformi alle Norme del programma per gli sviluppatori di Google Play; inoltre, se il pubblico di destinazione della tua app include bambini, assicurati di rispettare le nostre Norme per le famiglie.

Ricorda che è tua responsabilità esaminare il Contratto di distribuzione per gli sviluppatori e tutte le Norme del programma per gli sviluppatori per assicurare la piena conformità della tua app.

Developer Distribution Agreement

Hai bisogno di ulteriore assistenza?

Prova i passaggi successivi indicati di seguito:

Contattaci

Dacci ulteriori informazioni e potremo aiutarti