

# Norme del programma per gli sviluppatori

(in vigore dal 17 gennaio 2022, 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 con contenuti che sessualizzano i minori sono soggette alla rimozione immediata dallo Store, incluse, a titolo esemplificativo ma non esaustivo, le app che promuovono la pedofilia o l'interazione inappropriata indirizzata a un minore (ad esempio palpeggiamenti o carezze).

Inoltre, sono vietate le app che attirano i bambini, 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.

Se veniamo a conoscenza di contenuti con immagini pedopornografiche, li segnaliamo alle autorità competenti ed eliminiamo gli Account Google delle persone coinvolte nella distribuzione.

---

## 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 vietate le app o i contenuti delle app che sembrano promuovere atti sessuali in cambio di un compenso. I contenuti che includono nudità possono essere consentiti se il loro scopo principale è didattico, documentaristico, scientifico o artistico e tale nudità non è fine a se stessa.

Se un'app ha contenuti che violano queste norme, ma che sono ritenuti appropriati in un'area geografica specifica, l'app potrebbe essere disponibile per gli utenti dell'area geografica in questione, ma non sarà disponibile per gli utenti di altre aree geografiche.

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.

- 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 raffiguranti o che 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 pornografia con animali.

- App che promuovono servizi di intrattenimento sessuale, di escort o di altro tipo che potrebbero essere interpretati come un'offerta 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.

## Incitamento all'odio

Sono vietate le app che promuovono la violenza o incitano all'odio verso individui o gruppi di persone in base alla loro razza o etnia di origine, religione, disabilità, età, nazionalità, condizione di reduce di guerra, orientamento sessuale, genere, identità di genere o altre caratteristiche associate a discriminazione o emarginazione sistematica.

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

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 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.

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.

- 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.

## Contenuti di natura terroristica

Non consentiamo alle organizzazioni terroristiche di pubblicare app su Google Play per alcuno scopo, incluso il reclutamento.

Non sono ammesse app con contenuti correlati al terrorismo, ad esempio che promuovono atti terroristici, incitano alla violenza o celebrano attacchi terroristici. Per la pubblicazione di contenuti correlati al terrorismo a scopo didattico, documentaristico, scientifico o artistico è necessario fornire il contesto pertinente di tali contenuti.

## Organizzazioni e movimenti pericolosi

Non è consentito a movimenti oppure organizzazioni coinvolte in atti di violenza contro civili, che hanno preparato tali atti o ne hanno rivendicato la responsabilità, di pubblicare app su Google Play per alcuno scopo, incluso il reclutamento.

Non sono consentite app con contenuti correlati alla pianificazione, alla preparazione o alla glorificazione della violenza contro i civili. Se la tua app include contenuti di questo tipo a scopo didattico, documentaristico, scientifico o artistico, devi indicare il contesto pertinente.

## Eventi sensibili

Sono vietate le app che non manifestino la dovuta sensibilità nei confronti di calamità naturali, atrocità, crisi sanitarie, conflitti, decessi o altri eventi tragici, oppure che sfruttino tali eventi. Le app con contenuti correlati a un evento sensibile sono generalmente consentite se tali contenuti hanno un valore ai fini EDSA o intendono informare o

sensibilizzare le persone in merito all'evento.

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.

- 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 di un evento tragico di rilievo.
- Apparente derivazione di profitto da un evento tragico senza vantaggi evidenti per le vittime.
- Pubblicazione di app che violano le linee guida descritte nell'[articolo Requisiti per le app relative alla malattia da coronavirus 2019 \(COVID-19\)](#).

## Bullismo e molestie

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

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.

- 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.

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.

- 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 (incluse le sigarette elettroniche e i vaporizzatori a penna) o che incoraggiano l'uso illegale o inappropriato di alcol o tabacco.

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.

- Raffigurare o incoraggiare l'uso o la vendita di alcol o tabacco ai minori.
- Sottintendere che il consumo di tabacco possa migliorare le condizioni sociali, sessuali, professionali, intellettuali o atletiche.
- Raffigurare in una luce positiva l'eccessivo consumo di alcolici, inclusa la pratica del "binge drinking".

---

## Servizi finanziari

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

Nell'ambito 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 prodotti e servizi finanziari, è obbligatorio rispettare le normative statali e locali di ogni area geografica o paese di destinazione dell'app, ad esempio includendo dichiarazioni specifiche richieste dalla legge locale.

## Opzioni binarie

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

## Criptovalute

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

## Prestiti personali

Definiamo "prestito personale" l'atto occasionale di prestare denaro, da parte di una persona fisica, organizzazione o persona giuridica e a beneficio di un singolo consumatore, non destinato a finanziare l'istruzione personale o l'acquisto di immobilizzazioni. Per prendere decisioni informate in merito alla richiesta 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 diano informazioni esaurienti in merito alla visualizzazione, alla raccolta, all'utilizzo e alla condivisione dei dati utente personali e sensibili.

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").

### 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 terzi.

### Requisiti aggiuntivi relativi alle app per prestiti personali in India e Indonesia

Le app per prestiti personali in India e Indonesia devono essere conformi ai requisiti aggiuntivi di prova dell'idoneità che seguono.

#### 1. India

- Compila la [dichiarazione relativa alle app per prestiti personali per l'India](#) e fornisci la necessaria documentazione giustificativa. Ad esempio:
  - Se la Reserve Bank of India (RBI) ti ha autorizzato 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.
- Assicurati che il nome dell'account sviluppatore rifletta il nome dell'attività registrata associata fornito tramite la dichiarazione.

## 2. Indonesia

- Sono consentite soltanto le app per prestiti personali dotate di licenza dell'Autorità per i servizi finanziari dell'Indonesia (Otoritas Jasa Keuangan, "OJK") o registrate presso tale ente.
- Compila la [dichiarazione relativa alle app per prestiti personali per l'Indonesia](#) e fornisci la documentazione giustificativa dell'OJK.
- Assicurati che il nome dell'account sviluppatore rifletta il nome dell'attività registrata associata fornito tramite la dichiarazione.

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.

The screenshot shows the Google Play Store page for the app 'Easy Loans'. The app icon is a blue square with a white dollar sign. The title is 'Easy Loans' and it says 'offers in app purchases'. There is a green 'Install' button. Below the app name, there is a question: 'Are you looking for a speedy loan?' and a description: 'Easy Loans Finance can help you get cash in your bank account in an hour!'. A list of features is provided: 'Get cash sent to your bank account!', 'Safe and easy', 'Great short-term rate', 'Fast lender approval', 'Easy to use', 'Loan delivered in an hour', and 'Download our app and get cash easy!'. A red box with a white border and the word 'Violations' in a red box with a white border and an arrow pointing to it, highlights a red box containing the following text: 'No minimum and maximum period for repayment', 'Doesn't disclose Maximum Annual Percentage Rate (APR), which generally includes interest rate plus fees and other costs for a year, or similar other rate calculated consistently with local law', and 'No representative example of the total cost of the loan, including all applicable fees'.

## Giochi e scommesse

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 nei paesi indicati nella tabella che segue, 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 (consulta la tabella che segue per conoscere i tipi specifici di prodotti di giochi e scommesse consentiti in ogni paese):

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

---

## Australia

Riepilogo	Dettagli
Consentite con limitazioni	<p>Ai sensi dei requisiti relativi alla richiesta di iscrizione e alla licenza indicati in questa sezione "App di giochi e scommesse", sono ammesse le app con i seguenti tipi di prodotti di giochi e scommesse:</p> <ul style="list-style-type: none"><li>• Scommesse sportive (inclusi i fantasport giornalieri, nei paesi in cui sono legali)</li><li>• Lotterie</li></ul>

---

## Belgio

Riepilogo	Dettagli
Consentite con limitazioni	<p>Ai sensi dei requisiti relativi alla richiesta di iscrizione e alla licenza indicati in questa sezione "App di giochi e scommesse", sono ammesse le app con i seguenti tipi di prodotti di giochi e scommesse:</p> <ul style="list-style-type: none"><li>• Giochi da casinò online</li><li>• Scommesse sportive</li><li>• Lotterie (solo operatori statali)</li></ul>

---

## Brasile

Riepilogo	Dettagli
Consentite con limitazioni	<p>Ai sensi dei requisiti relativi alla richiesta di iscrizione e alla licenza indicati in questa sezione "App di giochi e scommesse", sono ammesse le app con i seguenti tipi di prodotti di giochi e scommesse:</p> <ul style="list-style-type: none"><li>• Scommesse sportive (solo corse di cavalli)</li><li>• Lotterie (limitatamente alle app approvate pubblicate dalla Caixa Economica Federal)</li></ul>

---

## Canada

Riepilogo	Dettagli
Consentite con limitazioni	<p>Ai sensi dei requisiti relativi alla richiesta di iscrizione e alla licenza indicati in questa sezione "App di giochi e scommesse", sono ammesse le app con i seguenti tipi di prodotti di giochi e scommesse:</p> <ul style="list-style-type: none"><li>• Giochi da casinò online (solo operatori statali)</li><li>• Scommesse sportive (solo operatori statali)</li><li>• Lotterie (solo operatori statali)</li></ul>

---

## Colombia

Riepilogo	Dettagli
Consentite con limitazioni	<p>Ai sensi dei requisiti relativi alla richiesta di iscrizione e alla licenza indicati in questa sezione "App di giochi e scommesse", sono ammesse le app con i seguenti tipi di prodotti di giochi e scommesse:</p> <ul style="list-style-type: none"><li>• Giochi da casinò online</li><li>• Scommesse sportive</li><li>• Lotterie (solo operatori statali)</li></ul>

---

---

## Danimarca

Riepilogo	Dettagli
Consentite con limitazioni	<p>Ai sensi dei requisiti relativi alla richiesta di iscrizione e alla licenza indicati in questa sezione "App di giochi e scommesse", sono ammesse le app con i seguenti tipi di prodotti di giochi e scommesse:</p> <ul style="list-style-type: none"><li>• Giochi da casinò online</li><li>• Scommesse sportive (inclusi i fantasport giornalieri, nei paesi in cui sono legali)</li><li>• Lotterie</li></ul>

---

## Finlandia

Riepilogo	Dettagli
Consentite con limitazioni	<p>Ai sensi dei requisiti relativi alla richiesta di iscrizione e alla licenza indicati in questa sezione "App di giochi e scommesse", sono ammesse le app con i seguenti tipi di prodotti di giochi e scommesse:</p> <ul style="list-style-type: none"><li>• Giochi da casinò online (solo operatori statali)</li><li>• Scommesse sportive (solo operatori statali)</li><li>• Lotterie (solo operatori statali)</li></ul>

---

## Francia

Riepilogo	Dettagli
Consentite con limitazioni	<p>Ai sensi dei requisiti relativi alla richiesta di iscrizione e alla licenza indicati in questa sezione "App di giochi e scommesse", sono ammesse le app con i seguenti tipi di prodotti di giochi e scommesse:</p> <ul style="list-style-type: none"><li>• Giochi da casinò online</li><li>• Scommesse sportive</li><li>• Corse di cavalli (se regolamentate e autorizzate con licenza separatamente dalle scommesse sportive)</li><li>• Lotterie (solo operatori statali)</li></ul>

---

## Germania

Riepilogo	Dettagli
Consentite con limitazioni	<p>Ai sensi dei requisiti relativi alla richiesta di iscrizione e alla licenza indicati in questa sezione "App di giochi e scommesse", sono ammesse le app con i seguenti tipi di prodotti di giochi e scommesse:</p> <ul style="list-style-type: none"><li>• Scommesse sportive</li><li>• Corse di cavalli (se regolamentate e autorizzate con licenza separatamente dalle scommesse sportive)</li><li>• Lotterie (solo operatori statali oppure operatori a contratto affiliati)</li></ul>

---

## Irlanda

Riepilogo	Dettagli
-----------	----------

---

Riepilogo	Dettagli
Consentite con limitazioni	<p>Ai sensi dei requisiti relativi alla richiesta di iscrizione e alla licenza indicati in questa sezione "App di giochi e scommesse", sono ammesse le app con i seguenti tipi di prodotti di giochi e scommesse:</p> <ul style="list-style-type: none"><li>• Giochi da casinò online</li><li>• Scommesse sportive</li><li>• Lotterie (solo operatori statali oppure organizzazioni benefiche)</li></ul>

---

## Giappone

Riepilogo	Dettagli
Consentite con limitazioni	<p>Ai sensi dei requisiti relativi alla richiesta di iscrizione e alla licenza indicati in questa sezione "App di giochi e scommesse", sono ammesse le app con i seguenti tipi di prodotti di giochi e scommesse:</p> <ul style="list-style-type: none"><li>• Scommesse sportive (gare di cavalli, motoscafi, biciclette, motociclette e partite di calcio, organizzate soltanto da operatori statali)</li><li>• Lotterie (solo operatori statali)</li></ul>

---

## Messico

Riepilogo	Dettagli
Consentite con limitazioni	<p>Ai sensi dei requisiti relativi alla richiesta di iscrizione e alla licenza indicati in questa sezione "App di giochi e scommesse", sono ammesse le app con i seguenti tipi di prodotti di giochi e scommesse:</p> <ul style="list-style-type: none"><li>• Giochi da casinò online</li><li>• Scommesse sportive</li><li>• Lotterie</li><li>• Fantasport giornalieri</li></ul>

---

## Nuova Zelanda

Riepilogo	Dettagli
Consentite con limitazioni	<p>Ai sensi dei requisiti relativi alla richiesta di iscrizione e alla licenza indicati in questa sezione "App di giochi e scommesse", sono ammesse le app con i seguenti tipi di prodotti di giochi e scommesse:</p> <ul style="list-style-type: none"><li>• Scommesse sportive (solo operatori statali)</li><li>• Lotterie (solo operatori statali)</li></ul>

---

## Norvegia

Riepilogo	Dettagli
Consentite con limitazioni	<p>Ai sensi dei requisiti relativi alla richiesta di iscrizione e alla licenza indicati in questa sezione "App di giochi e scommesse", sono ammesse le app con i seguenti tipi di prodotti di giochi e scommesse:</p> <ul style="list-style-type: none"><li>• Giochi da casinò online</li><li>• Scommesse sportive (solo operatori statali)</li><li>• Lotterie</li></ul>

---

---

## Romania

Riepilogo	Dettagli
Consentite con limitazioni	<p>Ai sensi dei requisiti relativi alla richiesta di iscrizione e alla licenza indicati in questa sezione "App di giochi e scommesse", sono ammesse le app con i seguenti tipi di prodotti di giochi e scommesse:</p> <ul style="list-style-type: none"><li>• Giochi da casinò online</li><li>• Scommesse sportive</li><li>• Lotterie (solo operatori statali)</li></ul>

---

## Spagna

Riepilogo	Dettagli
Consentite con limitazioni	<p>Ai sensi dei requisiti relativi alla richiesta di iscrizione e alla licenza indicati in questa sezione "App di giochi e scommesse", sono ammesse le app con i seguenti tipi di prodotti di giochi e scommesse:</p> <ul style="list-style-type: none"><li>• Giochi da casinò online</li><li>• Scommesse sportive (inclusi i fantasport giornalieri, nei paesi in cui sono legali)</li><li>• Corse di cavalli (se regolamentate e autorizzate con licenza separatamente dalle scommesse sportive)</li><li>• Lotterie (solo operatori statali)</li></ul>

---

## Svezia

Riepilogo	Dettagli
Consentite con limitazioni	<p>Ai sensi dei requisiti relativi alla richiesta di iscrizione e alla licenza indicati in questa sezione "App di giochi e scommesse", sono ammesse le app con i seguenti tipi di prodotti di giochi e scommesse:</p> <ul style="list-style-type: none"><li>• Giochi da casinò online</li><li>• Scommesse sportive</li><li>• Lotterie (solo operatori statali)</li></ul>

---

## Regno Unito

Riepilogo	Dettagli
Consentite con limitazioni	<p>Ai sensi dei requisiti relativi alla richiesta di iscrizione e alla licenza indicati in questa sezione "App di giochi e scommesse", sono ammesse le app con i seguenti tipi di prodotti di giochi e scommesse:</p> <ul style="list-style-type: none"><li>• Giochi da casinò online</li><li>• Scommesse sportive (inclusi i fantasport giornalieri, nei paesi in cui sono legali)</li><li>• Lotterie</li></ul>

---

## Stati Uniti

Riepilogo	Dettagli
-----------	----------

---

Riepilogo	Dettagli
Consentite con limitazioni	<p>Ai sensi dei requisiti relativi alla richiesta di iscrizione e alla licenza indicati in questa sezione "App di giochi e scommesse", sono ammesse le app con i seguenti tipi di prodotti di giochi e scommesse in alcuni stati in cui sono legali e hanno una licenza appropriata:</p> <ul style="list-style-type: none"> <li>• Giochi da casinò online</li> <li>• Scommesse sportive</li> <li>• Corse di cavalli (se regolamentate e autorizzate con licenza separatamente dalle scommesse sportive)</li> <li>• Lotterie</li> </ul> <p>Tieni presente che se uno stato o un prodotto di giochi e scommesse di uno stato non è disponibile nel <a href="#">modulo della richiesta di iscrizione</a>, significa che al momento Google Play non consente la distribuzione.</p> <p>In base allo stato, i fantasport giornalieri potrebbero essere regolamentati come giochi e scommesse negli Stati Uniti e tutte le app di fantasport giornalieri pubblicate negli Stati Uniti sono soggette ai requisiti relativi alle app di fantasport giornalieri (DFS) che seguono.</p>

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 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.

## 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, sono vietati 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 con elementi di 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.

## 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.

<b>Tipo di app con programma fedeltà</b>	<b>Programma fedeltà con elementi di gamification e premi variabili</b>	<b>Premi fedeltà basati su un rapporto o una programmazione fissi</b>	<b>Termini e condizioni obbligatori del programma fedeltà</b>	<b>I Termini e condizioni devono comunicare le probabilità o il metodo di selezione di qualsiasi programma fedeltà basato su probabilità</b>
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.

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.

- Agevolazione della vendita o dell'acquisto di sostanze stupefacenti illegali o di farmaci con obbligo di prescrizione medica senza prescrizione medica.
  - Raffigurazione o istigazione al consumo o alla vendita di droghe, alcol e tabacco ai 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 o accessibili ad almeno un sottoinsieme di utenti dell'app.

Le app che contengono o prevedono l'uso di contenuti generati dagli utenti devono:

- Richiedere agli utenti l'accettazione dei termini e condizioni d'uso dell'app e/o delle norme relative agli utenti prima che gli utenti possano creare o caricare contenuti di questo tipo;
- Definire contenuti e comportamenti discutibili (in modo conforme alle Norme del programma per gli sviluppatori di Play) e vietarli nei termini e condizioni d'uso o nei criteri relativi agli utenti dell'app;
- Implementare una funzionalità di moderazione dei contenuti generati dagli utenti che sia continua, efficace e robusta, nonché ragionevole e coerente rispetto al tipo o ai tipi di contenuti generati dagli utenti ospitato o ospitati dall'app;
  - Nel caso di app di live streaming, tutti i contenuti generati dagli utenti che siano discutibili devono essere rimossi idealmente in tempo reale e comunque non appena ragionevolmente possibile;
  - Nel caso di app in 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 siano discutibili (ad esempio, un'immagine AR sessualmente esplicita) sia della posizione di ancoraggio AR sensibile (ad esempio, contenuti AR ancorati a un'area geografica con restrizioni, come una base militare o una proprietà privata in cui l'ancoraggio AR potrebbe causare problemi al titolare della proprietà);
- Offrire un sistema in-app di facile utilizzo per la segnalazione di contenuti generati dagli utenti che siano discutibili e prendere provvedimenti nei confronti di tali contenuti, ove opportuno;
- Rimuovere o bloccare gli utenti molesti che violano i termini e condizioni d'uso dell'app e/o le norme relative agli utenti;
- Fornire misure di tutela per impedire che la monetizzazione in-app incoraggi comportamenti discutibili da parte degli utenti.

Le app il cui scopo principale è la pubblicazione di contenuti generati dagli utenti che siano discutibili saranno rimosse da Google Play. Analogamente, le app il cui fine è quello di essere utilizzate principalmente per ospitare contenuti discutibili generati dagli utenti, oppure di diventare note come luogo in cui prosperano tali contenuti, saranno rimosse da Google Play.

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.

- 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.
- 

## Sostanze non approvate

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

- Tutte le voci di questo elenco non esaustivo di [prodotti farmaceutici e integratori vietati](#)
- Prodotti contenenti efedra
- Prodotti contenenti gonadotropina corionica umana (hCG) in relazione alla perdita di peso o al 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 approvati da enti non autorizzati dalla legge, pubblicizzati in modo da implicarne la sicurezza o l'efficacia nel prevenire o curare una malattia o disturbo di 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](http://www.legitscript.com).

---

## 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.

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.

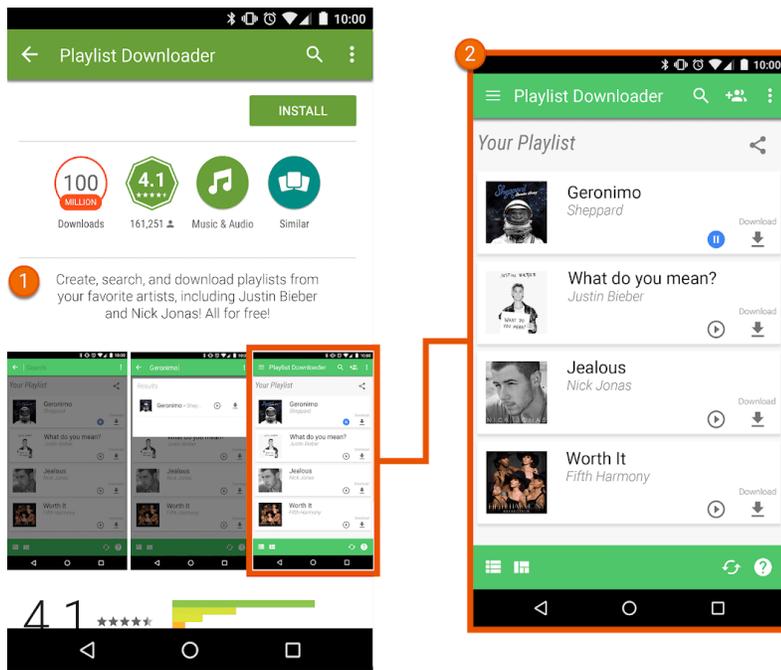
- Immagini di copertina di album musicali, videogiochi e libri.
- Immagini di marketing di film, programmi TV o videogiochi.
- Artwork o immagini di fumetti, cartoni animati, film, video musicali o programmi TV.
- Loghi di università e di squadre sportive professionali.
- Foto recuperate dall'account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

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.

- 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, sicurezza e comportamento ingannevole

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 (ovvero 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'app e limitare l'uso dei dati alle finalità comunicate. Inoltre, se l'app gestisce dati utente personali e sensibili, devi fare riferimento anche ai requisiti aggiuntivi indicati nella sezione "Dati utente personali e sensibili" di seguito. I presenti requisiti di Google Play si aggiungono ai requisiti previsti dalle leggi vigenti in materia di privacy e protezione dei dati. Se includi nell'app codice di terze parti (ad esempio SDK), devi assicurarti che sia conforme alle Norme del programma per gli sviluppatori di Google Play.

### 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, 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 scopi direttamente correlati alla fornitura e al miglioramento delle funzionalità dell'app (ad esempio, funzionalità anticipate all'utente che siano documentate e promosse nella descrizione dell'app su Google Play). La condivisione di dati utente personali e sensibili include l'uso di SDK o altri servizi di terze parti che causano il trasferimento di dati a una terza parte. Le app che estendono l'utilizzo dei dati utente personali e sensibili per la pubblicazione di annunci devono essere conformi alle nostre [norme relative agli annunci](#).
- 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, laddove disponibile, prima di accedere ai dati controllati tramite [autorizzazioni Android](#).
- Non devi vendere dati utente personali e sensibili.

### Requisito di consenso e visibilità dell'informativa

Nei casi in cui gli utenti potrebbero ragionevolmente non aspettarsi che i propri dati utente personali e sensibili siano richiesti per fornire o migliorare le funzionalità conformi alle norme o la funzionalità generale dell'app (ad esempio, la raccolta dei dati avviene in background), dovrai rispettare i seguenti requisiti:

**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.

**L'informativa in-app deve essere abbinata e precedere immediatamente una richiesta di consenso dell'utente e, laddove disponibile, un'autorizzazione di runtime associata. Non è permesso raccogliere dati personali e sensibili o accedere a tali dati senza il consenso dell'utente. 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; e
- Non deve utilizzare messaggi con scadenza o chiusura automatica per ottenere il consenso dell'utente.

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".*

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.

- 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 raccoglie 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.

:

### 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 <a href="#">Progettare app per bambini e famiglie</a> 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)	<p>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:</p> <ul style="list-style-type: none"> <li>servizi di telefonia collegati a un'identità SIM (ad esempio chiamate Wi-Fi collegate all'account di un operatore); e</li> <li>app di gestione di dispositivi aziendali, utilizzando la modalità proprietario del dispositivo.</li> </ul> <p>Questi utilizzi devono essere comunicati in posizione ben visibile, come specificato nelle <a href="#">norme relative ai dati utente</a>.</p> <p><a href="#">Consulta questa risorsa</a> per scoprire identificatori univoci alternativi.</p> <p>Leggi le <a href="#">norme relative agli annunci</a> per avere ulteriori indicazioni relative all'ID pubblicità di Android.</p>

In vigore dal 20 luglio 2022

### 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 sia nel relativo campo in Play Console sia 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 di Google Play dell'app oppure deve essere specificato il nome dell'app. Devono includere le norme sulla privacy anche le app che non accedono a dati utente personali e sensibili.

Assicurati che le norme sulla privacy siano disponibili su un URL attivo (non tramite PDF) e non possano essere modificate.

## 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](mailto: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

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 accedono a informazioni sensibili non possono mai essere venduti.

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 utente o del dispositivo sensibili a cui si accede tramite Autorizzazioni limitate possono essere trasferiti a terze parti esclusivamente se necessario per fornire o migliorare le funzionalità o i servizi esistenti nell'app da cui sono stati raccolti i dati. Puoi trasferire i dati anche come necessario per rispettare le leggi vigenti o nell'ambito di una fusione, un'acquisizione o una vendita di attività, fornendo agli utenti adeguato preavviso ai sensi di legge. Tutti gli altri tipi di trasferimenti o vendite dei dati utente sono vietati.
- 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.
- È espressamente vietato l'uso di autorizzazioni in violazione delle [best practice relative alle autorizzazioni app per sviluppatori Android](#) o delle norme esistenti, incluse le norme relative all'[abuso di privilegio elevato](#) .

Alcune autorizzazioni limitate potrebbero essere soggette a requisiti aggiuntivi, come descritto di seguito. L'obiettivo di queste restrizioni è tutelare la privacy degli utenti. Potremmo 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 richiede 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, 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.
- Impedire agli utenti di disattivare o disinstallare app o servizi.
- Aggirare le notifiche e i controlli per la privacy integrati in Android.
- Cambiare l'interfaccia utente o usarla in modo ingannevole o comunque con modalità che violano le norme per gli sviluppatori di Google Play.

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 il flag 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](#).

Le app devono usare [API e autorizzazioni](#) con ambito più limitato al posto dell'API Accessibility, ove possibile per ottenere la funzionalità desiderata.

---

## 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.

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.

- 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](#).
- App che facilitano servizi proxy verso terzi, comportamento consentito solo laddove questo sia lo scopo principale dell'app proposto all'utente.
- App o codice di terze parti (ad es. SDK) che scaricano codice eseguibile, come 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).

## Comportamento ingannevole

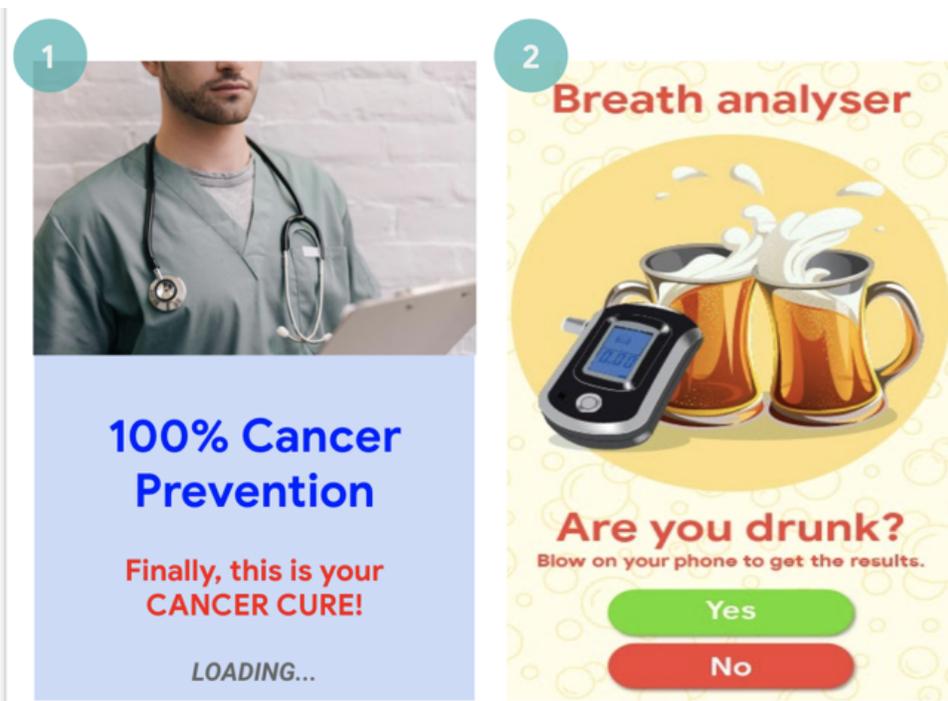
Sono vietate le app che cercano di ingannare gli utenti o di favorire comportamenti disonesti incluse, a titolo esemplificativo ma non esaustivo, tutte le app il cui funzionamento sia determinato essere impossibile. Le app devono contenere comunicazioni, descrizioni e immagini/video precisi relativi 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.

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.

- 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 con funzionalità o contenuti medici oppure relativi alla salute che sono ingannevoli o potenzialmente dannosi.
- App che dichiarano di avere funzionalità che in realtà non è possibile implementare, ad esempio app repellenti per gli insetti, anche se sono rappresentate come scherzi, imitazioni, prese in giro e così via.
- App classificate in modo errato inclusa, a titolo esemplificativo, la classificazione o la categoria dell'app.
- Contenuti falsi o manifestamente ingannevoli che potrebbero interferire con processi di voto.
- App che dichiarano, contrariamente al vero, un'affiliazione con entità governative o di offrire o agevolare servizi governativi per i quali non sono 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 mediche o relative alla salute (cura del cancro) ingannevoli

(2) Questa app dichiara di avere funzionalità che in realtà non è possibile implementare (uso del telefono 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 aiutino gli utenti a ingannare altri o che siano in qualsiasi modo ingannevoli dal punto di vista funzionale incluse, a titolo esemplificativo ma non esaustivo, app che generano o favoriscono la generazione di carte d'identità, codici fiscali, passaporti, diplomi, carte di credito e patenti di guida. Le app devono contenere comunicazioni, titoli, descrizioni e immagini/video accurati in relazione alla loro funzionalità e/o contenuti e funzionare secondo le ragionevoli e precise aspettative dell'utente.

È possibile scaricare risorse aggiuntive delle app (ad esempio, relative a giochi) solo quando 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.

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.

- 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, 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 un watermark, 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.

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.

- 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.

## 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.

## Malware

Le nostre norme sul 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.

Si definisce malware qualsiasi codice che potrebbe mettere a rischio un dispositivo, un utente o i suoi dati. Il termine malware include, a titolo esemplificativo, applicazioni potenzialmente dannose (PHA), programmi binari, modifiche di framework, appartenenti a varie categorie, ad esempio app di spyware, phishing o trojan. L'elenco delle categorie viene completato e aggiornato continuamente da Google.

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 e/o trasmette informazioni personali o sensibili dell'utente da un dispositivo senza adeguata comunicazione o consenso e non visualizza una notifica persistente in merito allo svolgimento di tale operazione.

Le app stalkerware scelgono come target gli utenti di dispositivi monitorando le informazioni personali o sensibili dell'utente e trasmettendo o rendendo tali dati accessibili a terze parti.

Purché soddisfino completamente i requisiti descritti di seguito, le app progettate e commercializzate esclusivamente per il monitoraggio dei figli da parte dei genitori o per la gestione aziendale sono le uniche app di sorveglianza accettabili. Tali app non possono essere utilizzate per monitorare altre persone che non siano i figli (ad esempio il coniuge) anche se con il loro consenso e la loro autorizzazione, a prescindere dalla visualizzazione di una notifica persistente.

Le app non stalkerware distribuite sul Play Store che monitorano o tengono traccia del comportamento di un utente su un dispositivo devono soddisfare quanto meno 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 tale funzionalità.
- Le app devono presentare agli utenti una notifica persistente per tutto il tempo quando un'app è in esecuzione e un'icona univoca che identifichi chiaramente l'app.
- 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.
- Sei l'unico responsabile della determinazione della legalità della tua app nel relativo paese di destinazione. Le app ritenute illegali nei paesi in cui vengono pubblicate verranno rimosse.

## 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

Codice che trasmette dati personali dal dispositivo senza un'adeguata comunicazione o consenso.

Ad esempio, la trasmissione di una qualsiasi delle seguenti informazioni senza comunicazione o in una modalità inaspettata per l'utente può essere già considerata spyware:

- Elenco contatti
- Fotografie o altri file provenienti dalla scheda SD o che non sono di proprietà dell'app
- Contenuti provenienti dall'email dell'utente
- Registro chiamate
- Registro SMS
- Cronologia web o preferiti del browser predefinito
- Informazioni provenienti dalle directory /data/ di altre app.

Possono essere definiti spyware anche comportamenti che possono essere considerati come spionaggio a danno dell'utente. Ad esempio, la registrazione di audio o di chiamate ricevute sul telefono o il furto di dati app.

## 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.

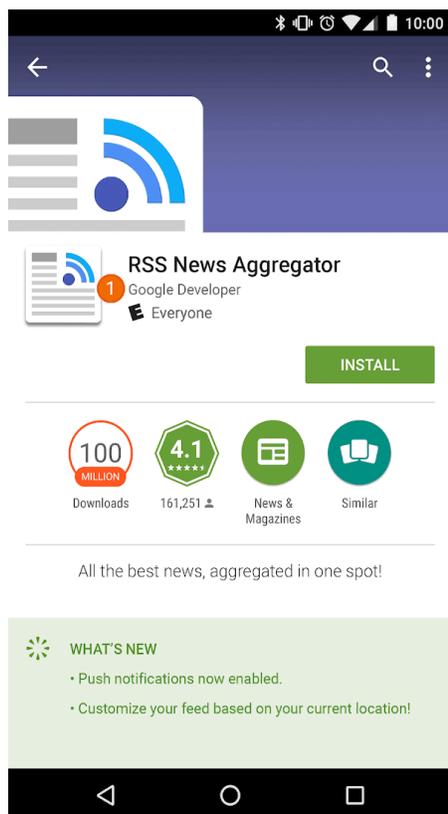
Tuttavia, se un'app consente l'esecuzione arbitraria di codice e non abbiamo ragione di credere che tale esecuzione sia stata aggiunta al fine di dar luogo a un comportamento malevolo, l'app verrà considerata come contenente una vulnerabilità, anziché essere definita malware backdoor, e allo sviluppatore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

## 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.

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.

- Sviluppatori che lasciano falsamente intendere l'esistenza di una relazione con un'altra azienda o sviluppatore:



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

- Titoli e icone di app molto simili a quelli di prodotti o servizi esistenti, che potrebbero trarre in inganno gli utenti:



- App che dichiarano di essere le app ufficiali di un'entità affermata, anche se in realtà non lo sono. 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](#).

## Mobile Unwanted Software

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 viola tali principi 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 viola 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
- Ingenuità sociale

## Proteggere i dati utente

*È necessario essere chiari e trasparenti in merito all'accesso, all'utilizzo, alla raccolta e alla condivisione di dati utente personali e sensibili. L'utilizzo dei dati utente deve rispettare tutte le Norme pertinenti relative ai dati utente, ove applicabili, e adottare tutte le misure necessarie per proteggere tali dati.*

- Lo sviluppatore deve fornire agli utenti l'opportunità di prestare il consenso alla raccolta dei loro dati prima di iniziare a raccogliervi e inviarli dal dispositivo, inclusi 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 per dispositivi mobili, deve trasmettere ai server dati utente personali e sensibili solo nella misura in cui siano correlati alla funzionalità dell'app.

Esempi di violazioni:

- Raccolta dei dati (vedere [Spyware](#))
- Utilizzo illecito di autorizzazioni limitate

Esempi di Norme sui dati utente:

- [Norme sui dati utente di Google Play](#)
- [Norme sui dati utente dei requisiti di Google Mobile Services](#)
- [Norme sui 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.

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.

- 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.

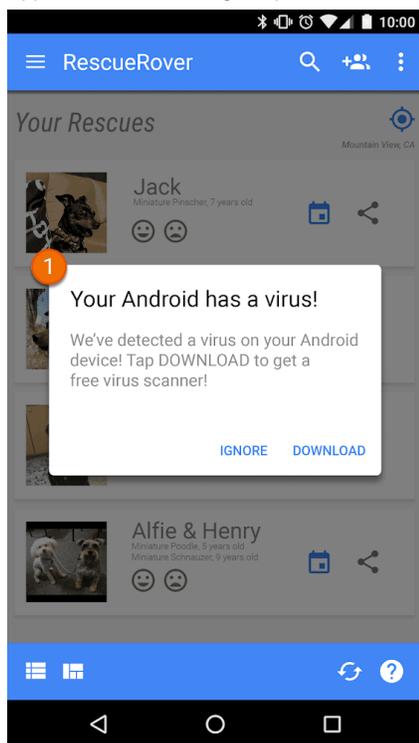
---

## 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.

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.

- 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](#).

---

## Social Engineering

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

---

Sono vietate le app contenenti annunci ingannevoli o improvvisi. Gli annunci possono essere visualizzati soltanto all'interno dell'app in cui vengono pubblicati. Gli annunci pubblicati nell'app vengono considerati parte dell'app e devono essere conformi a tutte le nostre norme. Fai clic [qui](#) per leggere le norme relative agli annunci di giochi e scommesse.

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 tali 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 tali transazioni, a meno che non si applichi la Sezione 3 o 8.

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 senza costi); 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 seguenti casi:

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 [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 e 8, le app non possono indirizzare gli utenti a un metodo di pagamento diverso dal sistema di fatturazione di Google Play. Tale 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 tali 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 tali articoli prima e in prossimità di tale acquisto.
8. A meno che non si applichino le condizioni descritte nella Sezione 3, gli sviluppatori di app per cellulari e tablet distribuite su Google Play che richiedono o accettano pagamenti degli utenti nella Corea del Sud per l'accesso agli acquisti in-app possono offrire agli utenti un sistema di fatturazione in-app oltre al sistema di fatturazione di Google Play per tali transazioni. A tale scopo devono compilare correttamente il [modulo di dichiarazione del sistema di fatturazione in-app aggiuntivo](#) e 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](#).

---

Sono vietate le app contenenti annunci ingannevoli o improvvisi. Gli annunci possono essere visualizzati soltanto all'interno dell'app in cui vengono pubblicati. Gli annunci pubblicati nell'app vengono considerati parte dell'app e devono essere conformi a tutte le nostre norme. Fai clic [qui](#) per leggere le norme relative agli annunci di giochi e scommesse.

Sono vietate le app contenenti annunci ingannevoli o improvvisi. Gli annunci possono essere visualizzati soltanto all'interno dell'app in cui vengono pubblicati. Gli annunci pubblicati nell'app vengono considerati parte dell'app e devono essere conformi a tutte le nostre norme. Fai clic [qui](#) per leggere le norme relative agli annunci di giochi e scommesse.

## 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:

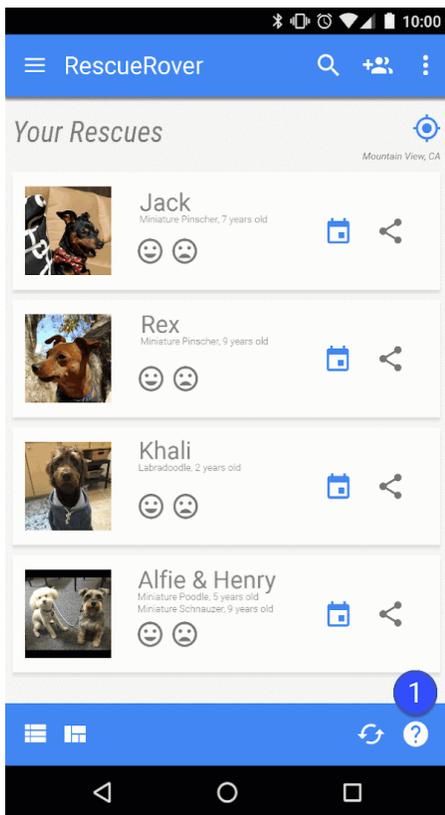
- L'utilizzo o la raccolta per scopi pubblicitari di dati sulla posizione del dispositivo basati sull'autorizzazione devono essere chiari all'utente e documentati nelle norme sulla privacy obbligatorie dell'app, incluso il collegamento a eventuali norme sulla privacy di reti pubblicitarie pertinenti, 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.

## Annunci ingannevoli

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

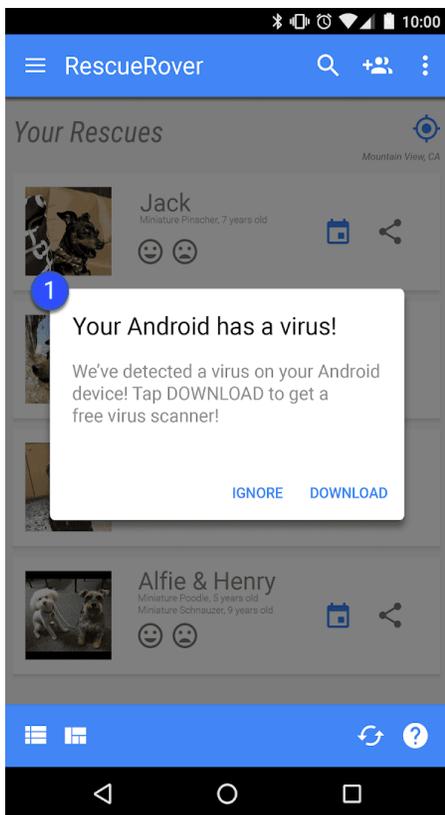
Per garantire che Google Play rimanga una piattaforma sicura e rispettosa, abbiamo creato degli standard che definiscono e proibiscono i contenuti dannosi o inappropriati per i nostri utenti.

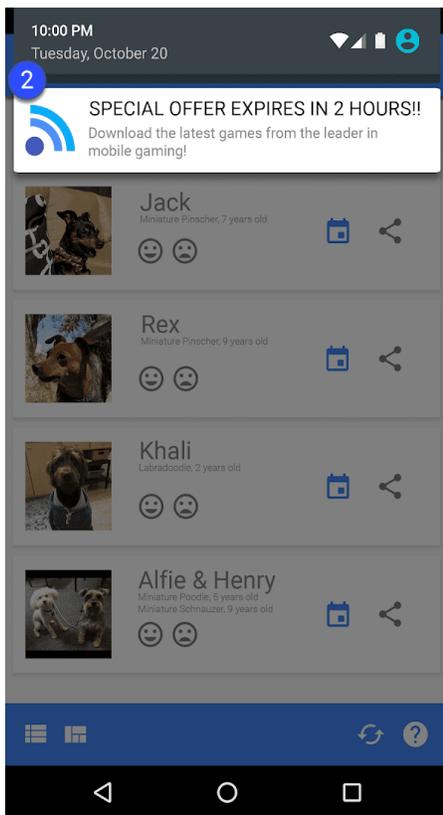
- Annunci che imitano l'interfaccia utente di un'app:



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.

## 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.

## Annunci improvvisi

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

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 interstitial possono essere mostrati solo all'interno dell'app che li pubblica. Se nell'app vengono mostrati annunci interstitial o altri annunci che interferiscono con il normale utilizzo, gli utenti devono poter ignorare facilmente gli annunci senza essere penalizzati.

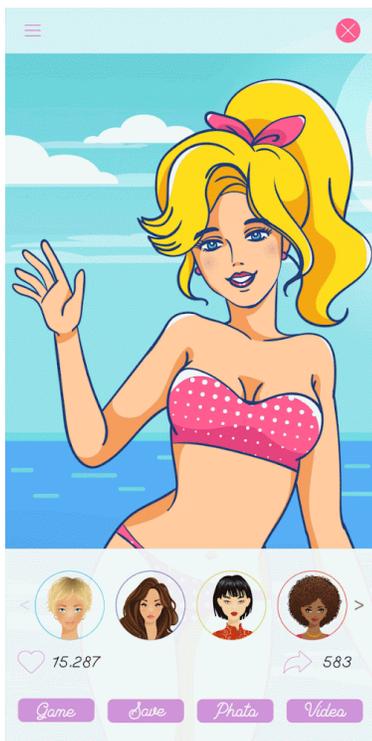
Per garantire che Google Play rimanga una piattaforma sicura e rispettosa, abbiamo creato degli standard che definiscono e proibiscono i contenuti dannosi o inappropriati per i nostri utenti.

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

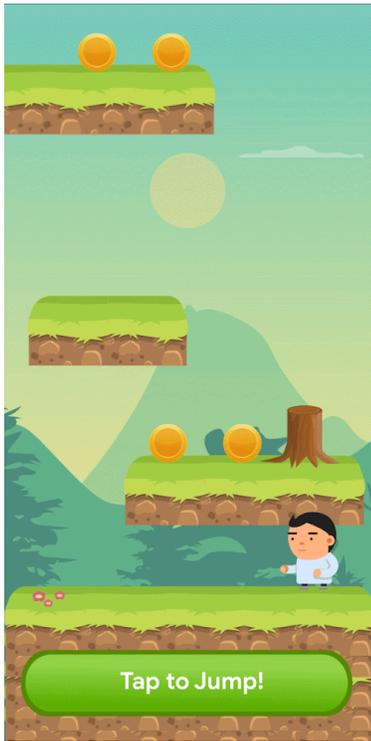


① Non è disponibile un pulsante per ignorare questo annuncio.

- 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.



- Un annuncio che utilizza un falso pulsante Ignora



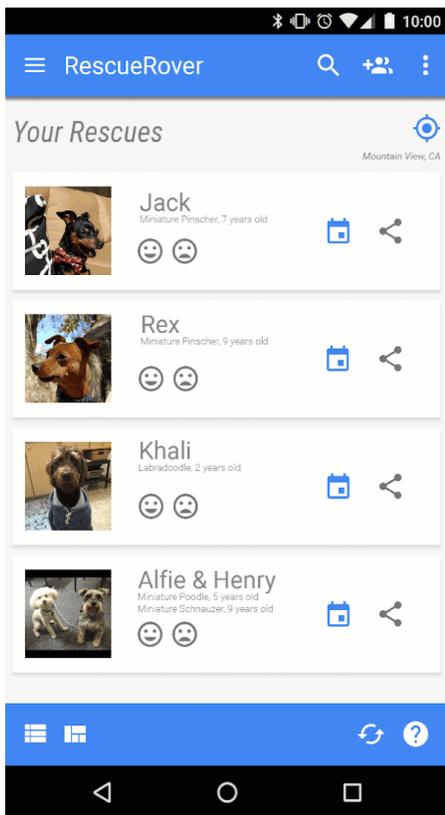
Un annuncio che appare all'improvviso in un'area che l'utente è abituato a toccare per accedere alle funzionalità in-app

## Interferenza con app, annunci di terze parti o funzionalità del dispositivo

Gli annunci associati all'app 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. Gli annunci possono essere visualizzati soltanto all'interno dell'app in cui vengono pubblicati.

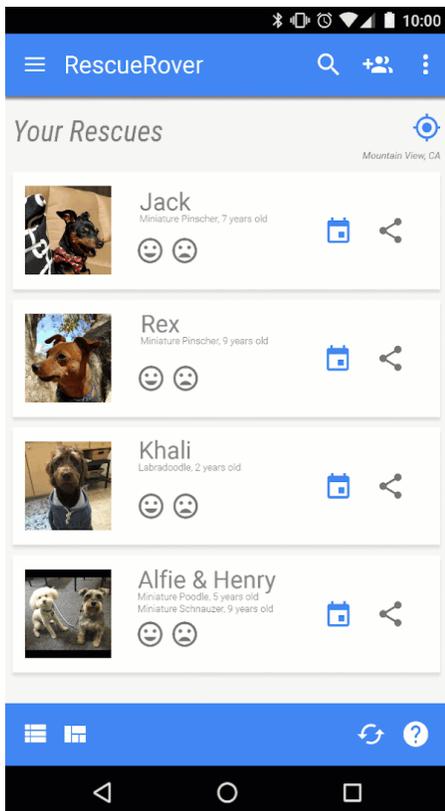
Per garantire che Google Play rimanga una piattaforma sicura e rispettosa, abbiamo creato degli standard che definiscono e proibiscono i contenuti dannosi o inappropriati per i nostri utenti.

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



Descrizione: l'utente passa alla schermata Home dall'app e sulla schermata Home viene improvvisamente visualizzato un annuncio.

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

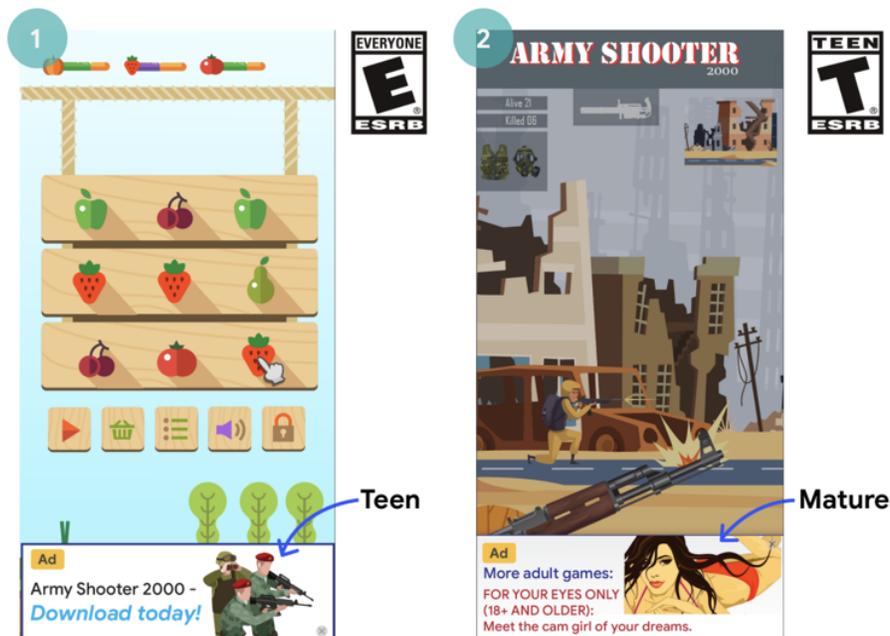


Descrizione: l'utente cerca di uscire dall'app e di accedere alla schermata Home, ma il flusso previsto viene interrotto da un annuncio.

## Annunci inappropriati

Gli annunci mostrati nell'app devono essere adatti al pubblico previsto dell'app, a prescindere dalla conformità dei contenuti alle norme di Google.

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.



① Questo annuncio non è appropriato (adolescenti) per il pubblico previsto dell'app (7+)

② Questo annuncio non è appropriato (adulti) per il pubblico previsto dell'app (12+)

## 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 dati analitici. 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 dei dispositivi persistenti (ad esempio, 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 può essere collegato solo a informazioni che consentono l'identificazione personale o associato a un identificatore del dispositivo persistente (ad esempio, indirizzo MAC, IMEI e così via) con il consenso esplicito dell'utente. Leggi le [norme sui dati utente](#) per maggiori linee guida sugli identificatori dei dispositivi 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 ammesse, ad esempio, la pubblicità contestuale, le quote limite, il monitoraggio delle conversioni, la creazione di rapporti e il 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 mostrerà una stringa di zeri. Un dispositivo privo di identificatore pubblicità non deve essere connesso ai dati collegati a un precedente identificatore pubblicità o da questo 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 un'Informativa sulla privacy legalmente adeguata. Per ulteriori informazioni sui nostri standard relativi alla privacy, leggere 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 condividi eventualmente nel corso della tua attività. Per tutte le app caricate o pubblicate su Google Play è necessario utilizzare l'ID pubblicità (se disponibile sul dispositivo) anziché qualsiasi altro identificatore del dispositivo per qualunque finalità pubblicitaria.
- 

## 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.

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.

- 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:

**Get AnalyzeAPP Premium**

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

<p><b>2</b> 12 months</p> <p>\$9.16/mo</p> <p>Save 35%!&lt;\/p&gt; </p>	<p><b>6 months</b></p> <p>\$12.50/mo</p> <p>Save 11%!&lt;\/p&gt; <p>MOST POPULAR PLAN</p> </p>	<p><b>1 month</b></p> <p>\$14.00/mo</p>
---	--	---

**3** Try for \$12.50!

**4** Cancele su suscripción en cualquier momento. Por favor, consulte nuestra política de privacidad para más información.

- 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:

**Start every day with a new lesson**

Learn calming techniques to ease your stress and start your day with calm.

CONTINUE

**Lots of choices to choose from**

Over 1,000 lessons and songs in the library for you to browse.

CONTINUE

**Share on social media**

Celebrate milestones by sharing with family and friends on social media.

CONTINUE

**1** PER MONTH USE 10.99/month

**3-DAY FREE TRIAL (FREE!)**  
THEN USD \$9.99/year

Free trials get charged after 3 days for the above price, non-free trials are charged immediately. You may cancel your free trial at any time before it expires to avoid charges by going to your Google Play account subscription settings. Subscription is required to use app. All sales are FINAL. We offer different packages from \$9.99/month all the way to the premier deluxe \$9.99/week. By signing up you agree to terms

CONTINUE

**Get AnalyzeAPP Premium**



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

**Start your 3-day FREE trial now!**

**★ Try for free now!**

**2** Then 26.99/month, cancel anytime

During your free trial, experience all of the great features our app can offer!

- 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.

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.

- 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.

**Get AnalyzeAPP Premium**

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

**Try for free now!**

3 During your free trial, experience all of the great features our app can offer!

4 Cancele su suscripción en cualquier momento. Por favor, consulte nuestra política de privacidad para más información.

- 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 e annullamento dell'abbonamento

In qualità di sviluppatore, devi assicurarti che le tue app indichino chiaramente in che modo gli utenti possono gestire o annullare il loro abbonamento.

Se un utente annulla un abbonamento acquistato da un'app su Google Play, le norme 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 responsabilità dello sviluppatore informare gli utenti in merito a eventuali modifiche apportate alle norme su abbonamento, annullamento e rimborsi e assicurarsi che tali norme siano conformi alla legge vigente.

## Programma relativo agli annunci per la famiglia

Se nell'app vengono visualizzati annunci e il pubblico di destinazione dell'app medesima include unicamente bambini e ragazzi come descritto nelle [Norme per le famiglie](#), è necessario utilizzare SDK di annunci che dispongono dell'autocertificazione di conformità con le norme di Google Play, inclusi i requisiti di certificazione per gli SDK di annunci indicati di seguito. Se il pubblico di destinazione dell'app è costituito da bambini e ragazzi e da utenti di età più elevata, è necessario implementare misure di controllo dell'età e assicurarsi che gli annunci mostrati a bambini e ragazzi provengano esclusivamente da uno degli SDK di annunci autocertificati. Per le app del programma Per la famiglia è necessario utilizzare soltanto SDK di annunci autocertificati.

L'uso di SDK di annunci certificati Google Play è richiesto soltanto se gli SDK di annunci sono utilizzati per mostrare annunci a bambini e ragazzi. Quanto indicato di seguito è consentito senza obbligo di autocertificazione degli SDK di annunci con Google Play, ma lo sviluppatore rimane responsabile di garantire che i contenuti degli annunci e le procedure di raccolta dei dati siano conformi alle [Norme relative ai dati utente di Play](#) e alle [Norme per le famiglie](#):

- Annunci autopromozionali quando gli SDK vengano utilizzati per gestire la promozione incrociata delle app dello sviluppatore o per altri contenuti multimediali di proprietà e merchandising
- Stipulazione di direct deal con gli inserzionisti qualora tu utilizzi SDK per la gestione dell'inventario

#### Requisiti di certificazione degli SDK di annunci

- Definire il contenuto dell'annuncio e i comportamenti discutibili e vietarli nei termini o nelle norme dell'SDK di annunci. Le definizioni devono essere conformi alle Norme del programma per gli sviluppatori di Google Play.
- 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 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. Tale trattamento deve essere conforme alle leggi e ai regolamenti vigenti, come la [normativa statunitense Children's Online Privacy and Protection Act \(COPPA\)](#) e il [Regolamento generale sulla protezione dei dati \(GDPR\)](#) dell'UE. Google Play richiede agli SDK di annunci di disattivare 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 per le famiglie e alla monetizzazione](#) di Play e che soddisfano 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 propagati agli offerenti.
- Fornisci a Google informazioni sufficienti, come quelle indicate nel [modulo di interesse](#) riportato di seguito, per verificare la conformità dell'SDK di annunci a tutti i requisiti di certificazione e rispondere tempestivamente a eventuali richieste successive di informazioni.

*Nota: gli SDK di annunci devono supportare la pubblicazione di annunci conformi a tutte le leggi e i regolamenti pertinenti relativi a bambini e ragazzi che possano applicarsi ai rispettivi publisher.*

Requisiti di mediazione delle piattaforme di pubblicazione di annunci destinati ai minori:

- Utilizzare solo SDK di annunci certificati Google Play o implementare le misure di protezione necessarie per garantire che tutti gli annunci pubblicati dalle reti di mediazione siano conformi a tali requisiti; e inoltre
- Trasmettere 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.

Gli sviluppatori possono consultare un [elenco di SDK di annunci autocertificati](#) qui.

Inoltre, gli sviluppatori possono condividere questo [modulo di interesse](#) con gli SDK di annunci per cui 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.

Esempi di violazioni comuni:

- 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.

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

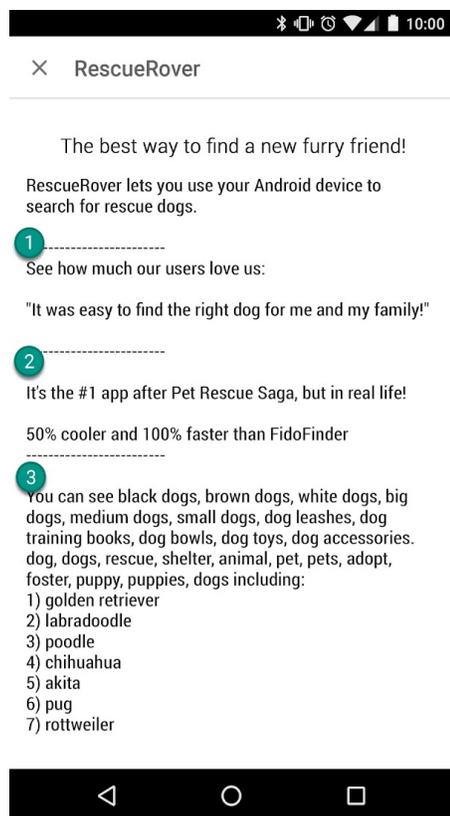
## Metadati

Sono vietate le app contenenti metadati fuorvianti, non correttamente formattati, non descrittivi, irrilevanti, eccessivi o inappropriati che siano presenti, 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.

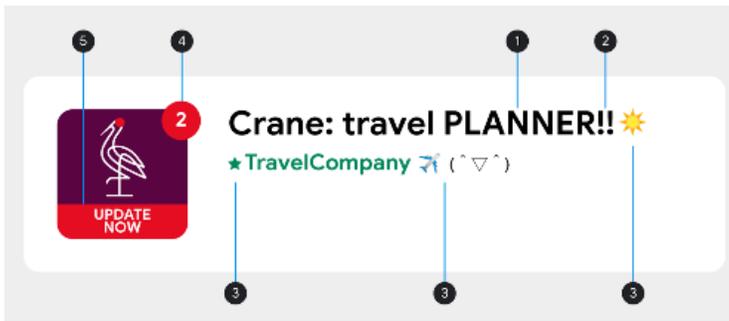
Il titolo e l'icona dell'app, nonché il nome dello sviluppatore, sono particolarmente utili per consentire agli utenti di trovare la tua app e acquisire informazioni in merito. Non usare emoji, emoticon o caratteri speciali ripetuti in questi elementi dei metadati. Evita di usare parole TUTTE MAIUSCOLE, 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.

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

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.



- 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

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.

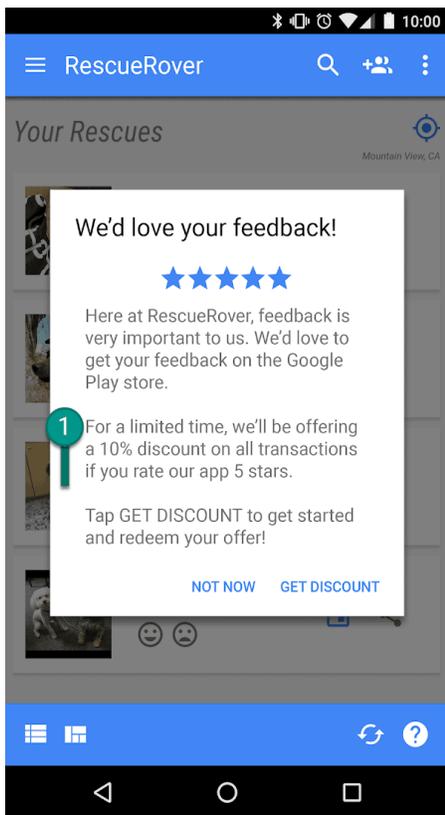
## Valutazioni, recensioni e installazioni degli utenti

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 installazioni, recensioni e valutazioni fraudolente o basate sull'offerta di incentivi. L'incentivazione di installazioni, recensioni e valutazioni include l'uso di testo o immagini nell'icona o nel titolo dell'app o nel nome sviluppatore che indichino il prezzo o altre informazioni promozionali.

Gli sviluppatori non devono aggiungere testo o immagini che indichino le prestazioni o il ranking sullo store, né suggerire collegamenti con programmi di Google Play esistenti nell'icona o nel titolo dell'app o nel nome sviluppatore.

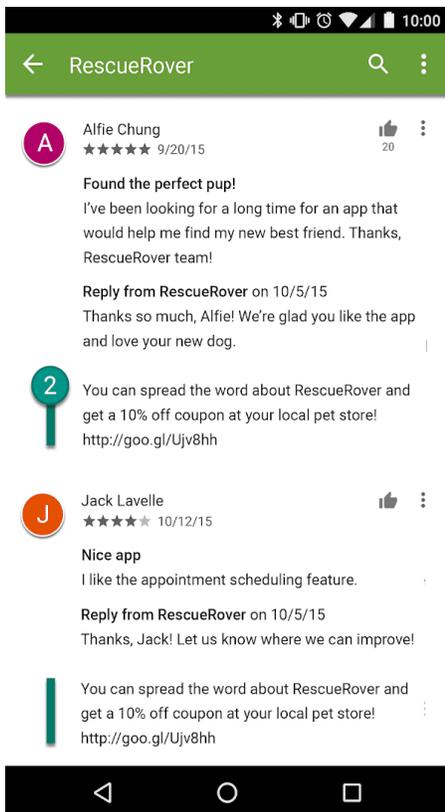
Per garantire che Google Play rimanga una piattaforma sicura e rispettosa, abbiamo creato degli standard che definiscono e proibiscono i contenuti dannosi o inappropriati per i nostri utenti.

- 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 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 benchmark 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.

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.

- 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.



**It's Magic - #1 in magic games**

Top Free Games.  
4.5 ★



**Music Player - Best of Play**

Super Play.  
4.5 ★



**Jackpot - Best Slot Machine**

Slot Games.  
4.5 ★



**Rewards Game**

RT Games.  
3.5 ★

- 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.



**O Basket - \$50 Cashback**

Digital Brand.  
4.5 ★



**Gmart - On Sale For Limited Time**

Shop Limited.  
4.3 ★



**Fish Pin- Free For Limited Time Only**

Entertainment Play.  
4.5 ★



**Golden Slots Fever: Free 100**

Gamepub Play.  
4.2 ★

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



**Build Roads - New Game**

KDG Games.  
3.5 ★



**Robot Game - Editor's choice**

Entertainment Games.  
4.5 ★

---

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 varie [autorità di classificazione](#) e su come completare il questionario relativo alla 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 che si autodefinisce di "notizie" in Play Console ("app di notizie") deve rispettare tutti i requisiti che seguono.

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'editore giornalistico e ai suoi collaboratori inclusi, a titolo esemplificativo, il sito web ufficiale delle notizie pubblicate nell'app, informazioni di contatto valide e verificabili e l'editore originale di ogni articolo; e
- Avere una pagina dedicata nell'app o nel sito web che indica chiaramente di contenere informazioni 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 informazioni di contatto valide dell'editore giornalistico. Tali informazioni devono includere almeno un indirizzo email e un numero di telefono di contatto.

Tieni presente che i link ad account di social media non sono informazioni di contatto degli editori sufficienti. Inoltre, le app che includono principalmente contenuti generati dagli utenti (ad esempio le app di social media) non devono autodefinirsi app di notizie.

Le app di notizie NON DEVONO:

- Contenere errori ortografici o grammaticali significativi;
- Avere soltanto contenuti statici (ad esempio contenuti risalenti a diversi mesi prima della data corrente); e
- 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 e funzionalità minima

Le app devono fornire agli utenti almeno un livello di funzionalità di base e un'esperienza utente accettabile. Le app che si bloccano, presentano altri comportamenti non coerenti con un'esperienza utente funzionale o che servono solo per mandare spam agli utenti o a Google Play non sono considerate app che ampliano il catalogo in modo costruttivo.

## Spam

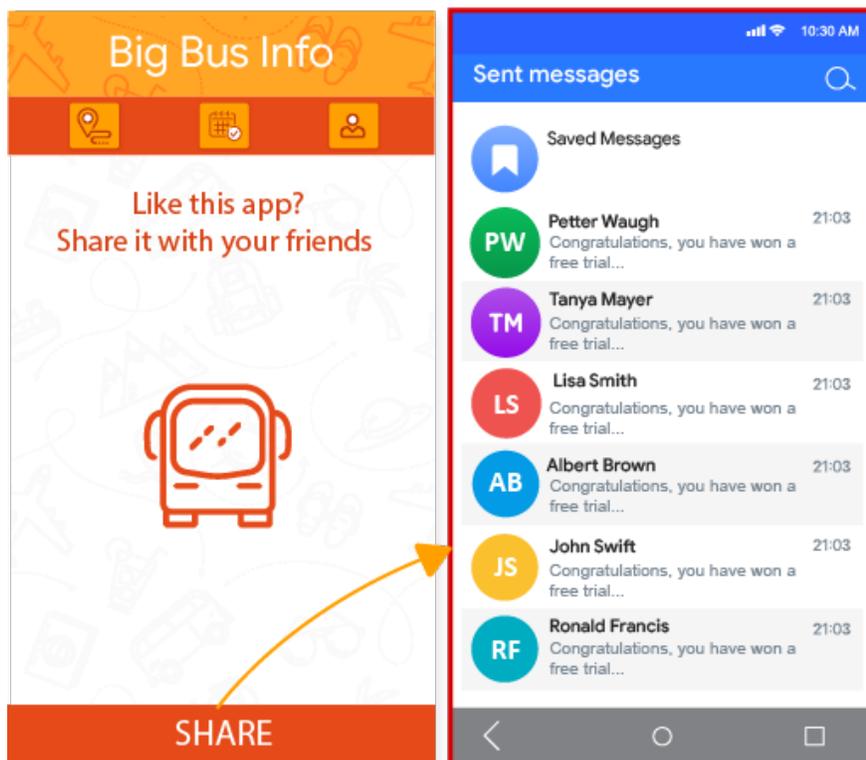
Sono vietate le app che inviano spam agli utenti o inseriscono spam su Google Play, ad esempio le app che inviano messaggi indesiderati agli utenti oppure le app duplicate o di scarsa qualità.

## 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.

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.

- 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:



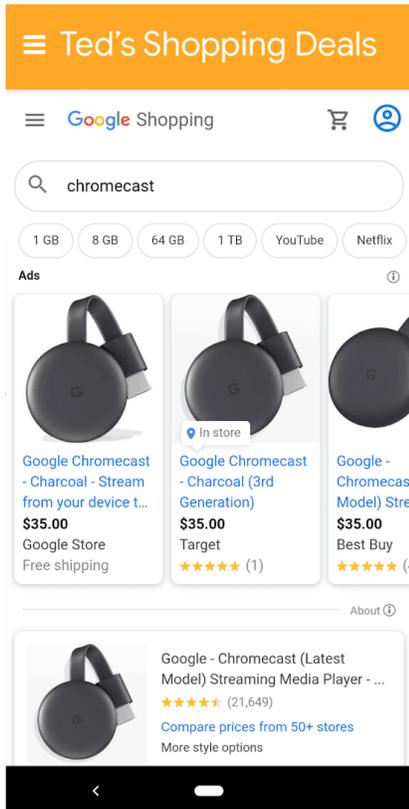
## Spam legato alle visualizzazioni web e per promuovere traffico affiliato

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.

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.

- 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:



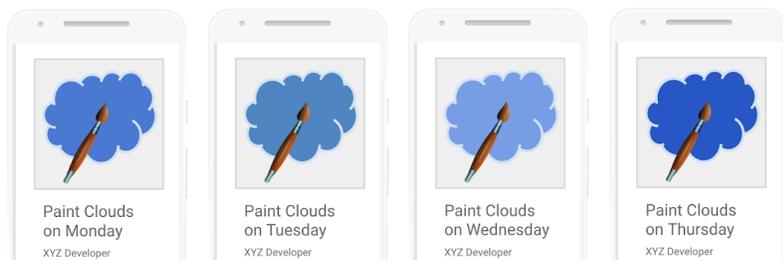
① Questa app è denominata "Ted's Shopping Deals" e fornisce semplicemente una visualizzazione web di Google Shopping.

## 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.

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.

- 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.



## App realizzate appositamente per gli annunci

Sono vietate le app il cui scopo principale è pubblicare annunci.

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.

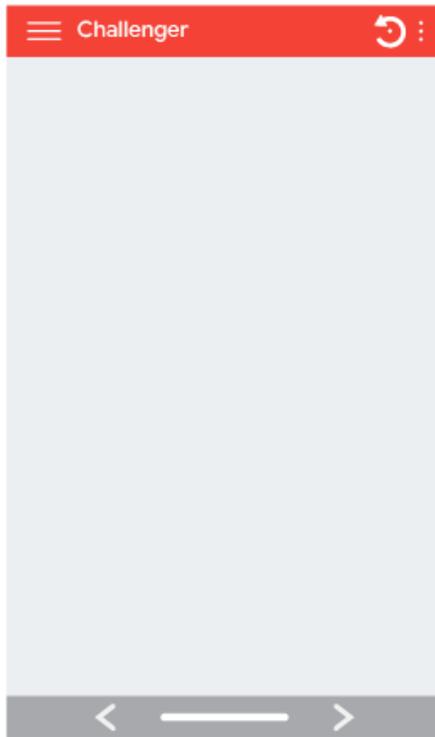
- Le app in cui vengono inseriti annunci interstitial dopo ogni azione dell'utente inclusi, a titolo esemplificativo, clic, scorrimenti e così via.

## Funzionalità minima

Assicurati che la tua app fornisca un'esperienza utente stabile, coinvolgente e reattiva.

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.

- App progettate per non fare nulla o per non avere alcuna funzione



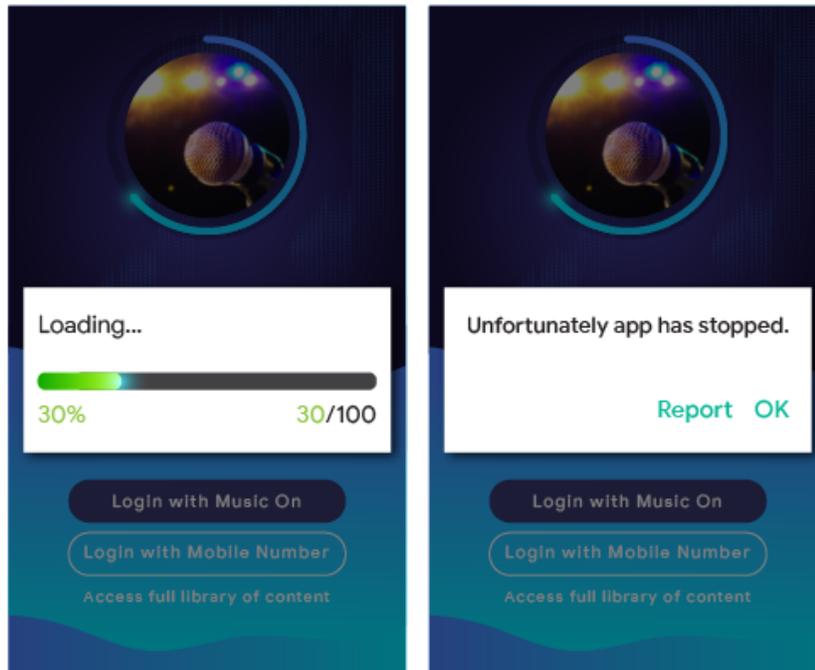
## Funzioni inaccessibili

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

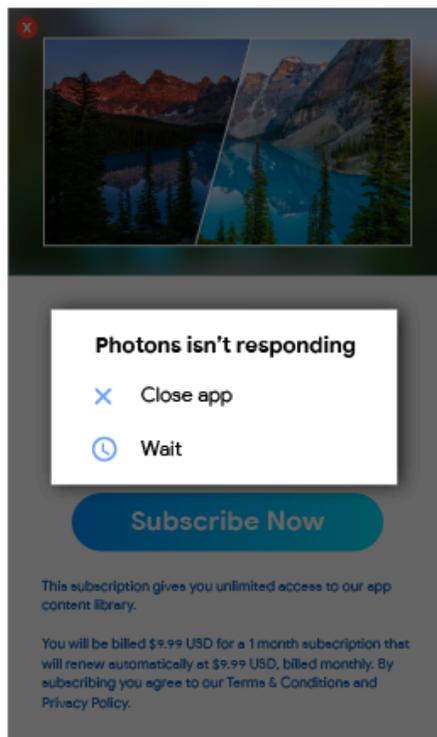
Per garantire che Google Play rimanga una piattaforma sicura e rispettosa, abbiamo creato degli standard che definiscono e proibiscono i contenuti dannosi o inappropriati per i nostri utenti.

- 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.

In vigore dall'11 maggio 2022

## Norme Android relative alle emoji

Le nostre norme relative alle emoji sono state pensate per promuovere un'esperienza utente inclusiva e uniforme sull'intera piattaforma Google.

Le app supportate su Android 12 e versioni successive dovranno conformarsi alla versione Unicode più recente entro 4 mesi dalla data in cui diventino disponibili pubblicamente.

Per mantenere la conformità costante delle app, gli sviluppatori DEVONO attenersi a una delle seguenti opzioni:

- Se è già in uso [AppCompat](#), assicurati che la voce emoji sia attiva.
- Usa una libreria [EmojiCompat](#) esistente in tutte le aree all'interno dell'app. Dovrebbe funzionare con le visualizzazioni personalizzate che usano direttamente [StaticLayout](#).
- Aggiorna la gestione del carattere/delle immagini relativi alle emoji in base all'ultima versione di Unicode.

Usa le emoji di esempio che seguono per verificare se l'app è conforme all'ultima versione di Unicode:

Esempi	Versione Unicode
	13.1
	13.0
	12.1
	12.0

Consulta [questa risorsa](#) per avere ulteriori indicazioni relative alla compatibilità delle emoji.

## 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.](#)

## Progettare app per bambini e famiglie

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 i bambini oppure potrebbero attirare semplicemente la loro attenzione. Google Play aiuterà a garantire che siano sicure per tutti gli utenti, comprese le famiglie.

Il termine "bambino" può assumere significati diversi a seconda dei paesi e dei contesti. È importante rivolgersi a un consulente legale che ti aiuti a determinare gli eventuali obblighi e/o le restrizioni in base alle fasce d'età applicabili alla propria 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.

Le app progettate specificatamente per i bambini devono partecipare al programma Per la famiglia. Se la tua app si rivolge sia ai bambini sia a segmenti di pubblico di età più elevata, puoi comunque partecipare al programma Per la famiglia. Tutte le app che partecipano al programma Per la famiglia saranno idonee a essere classificate per il , ma non possiamo garantire che verranno incluse nel programma. Se opti per non partecipare al programma Per la famiglia, devi comunque rispettare i requisiti delle Norme per le famiglie di Google Play riportati di seguito, così come tutte le altre [Norme del programma per gli sviluppatori di Google Play](#) e il [Contratto di distribuzione per gli sviluppatori](#).

## 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.

Nel caso in cui selezioni un pubblico di destinazione che include solo gli adulti, ma Google ritenga tale indicazione non corretta perché l'app ha come target anche i bambini, avrai la possibilità di chiarire agli utenti che la tua app non è destinata ai bambini accettando di mostrare un'etichetta di avviso.

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 relativi alle norme sulle famiglie

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

- 1. Contenuti dell'app:** i contenuti della tua app accessibili ai bambini devono essere adeguati per questi ultimi.
- 2. Funzionalità dell'app:** l'app non deve limitarsi a fornire una WebView di un sito web, né avere come obiettivo principale l'indirizzamento di traffico affiliato a un sito web, a prescindere dalla proprietà di quest'ultimo.
  - Siamo costantemente alla ricerca di metodi per rendere possibili nuove esperienze agli sviluppatori di app per bambini. Se ti interessa partecipare al nostro progetto pilota Trusted Web App per app per l'istruzione, comunicacelo [qui](#).
- 3. Risposte di Google Play Console:** devi rispondere con precisione alle domande relative alla tua app contenute in Play Console e aggiornare tali risposte in base a qualsiasi modifica apportata all'app. È inclusa, a titolo esemplificativo, la comunicazione precisa degli elementi interattivi dell'app nel questionario per la classificazione dei contenuti, ad esempio:
  - Gli utenti dell'app possono interagire o scambiarsi informazioni.
  - L'app condivide informazioni fornite dagli utenti con terze parti.
  - L'app condivide la posizione fisica dell'utente con altri utenti.
- 4. Annunci:** se la tua app visualizza annunci per bambini e ragazzi o utenti di età sconosciuta, devi:
  - Utilizzare solo [SDK di annunci certificati Google Play](#) per mostrare annunci a tali utenti;
  - Garantire che gli annunci mostrati a tali 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 tali utenti presentino contenuti appropriati per bambini e ragazzi;
  - Garantire che gli annunci mostrati a tali utenti rispettino i requisiti relativi al formato degli annunci per le famiglie; e inoltre
  - Assicurare la conformità a tutte le normative legali e gli standard di settore applicabili in materia di pubblicità destinata ai bambini.
- 5. 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:

- Non devi trasmettere identificatore pubblicità di Android (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 destinate esclusivamente a bambini e ragazzi non possono richiedere, raccogliere, usare o trasmettere la posizione.
- Le app devono utilizzare [Gestione dispositivi companion \(CDM\)](#) quando richiedono il Bluetooth, a meno che l'app non sia destinata solo a versioni di sistema operativo dei dispositivi non compatibili con CDM.

**6. 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. Ciò include il servizio Accedi con Google (o qualsiasi altro servizio API di Google che acceda ai dati associati a un Account Google), i servizi per i giochi di Google Play e qualsiasi altro servizio API che utilizzi la tecnologia OAuth per l'autenticazione e l'autorizzazione.
- 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 tramite un'API o un SDK non approvati per l'utilizzo nei servizi rivolti ai minori.

**7. 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).

**8. 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 Google Play Console.

- Applicazioni social: un'applicazione 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 applicazioni social con un pubblico di destinazione che comprende bambini e ragazzi è necessario fornire un promemoria in-app che ricordi di muoversi in sicurezza online e il rischio nel mondo reale che comporta l'interazione online prima di consentire a bambini e ragazzi di scambiare informazioni o contenuti multimediali in formato libero. 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 è necessario fornire un promemoria in-app che ricordi di muoversi in sicurezza online e il rischio nel mondo reale che comporta l'interazione online prima di consentire a bambini e ragazzi di scambiare informazioni o contenuti multimediali in formato libero. 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 tale 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 applicazioni 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.

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

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.

- 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 ai bambini.
- 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 ai bambini annunci destinati a un pubblico adulto (ad esempio, contenuti violenti, di natura sessuale o collegati a giochi e scommesse). Per ulteriori informazioni sulle Norme di Google Play relative alla pubblicità, agli acquisti in-app e ai contenuti commerciali destinati ai minori, consulta le [norme relative agli Annunci per le famiglie e alla monetizzazione](#).

## Programma Per la famiglia

Le app progettate specificatamente per i bambini devono partecipare al programma Per la famiglia. Se l'app è progettata per tutti, compresi bambini, ragazzi e famiglie, puoi comunque presentare domanda per partecipare al programma.

Per poter essere accettata nel programma, l'app deve essere conforme a tutti i requisiti delle Norme per le famiglie e a tutti i requisiti di idoneità del programma Per la famiglia, oltre a quelli indicati nelle [Norme del programma per gli sviluppatori di Google Play](#) e nel [Contratto di distribuzione per gli sviluppatori](#).

Per ulteriori informazioni sulla procedura per l'invio dell'app per l'inclusione nel programma, fai clic [qui](#).

### Idoneità al programma

I contenuti delle app che partecipano al programma Per la famiglia, compresi i contenuti degli annunci, devono essere pertinenti e adatti a bambini e ragazzi (le app devono avere la classificazione ESRB "Per tutti", "Per tutti 10+" o equivalente). Inoltre, le app devono usare soltanto [SDK di annunci certificati Google Play](#). Le app accettate per la partecipazione al programma Per la famiglia devono essere sempre conformi a tutti i requisiti del programma. Google Play può rifiutare, rimuovere o sospendere qualsiasi app ritenuta non appropriata al programma Per la famiglia.

### Di seguito sono riportati alcuni esempi di app comuni non idonee per il programma:

- App con classificazione ESRB Per tutti, ma con annunci relativi a contenuti di giochi e scommesse
- App per genitori o tutori (ad esempio tracker per l'allattamento al seno o guide allo sviluppo)
- Guide per i genitori o app di gestione dei dispositivi destinate esclusivamente a genitori o tutori

### Categorie

Se vieni ammesso a partecipare al programma Per la famiglia potrai scegliere una seconda categoria specifica del programma che descriva l'app. Di seguito vengono indicate le categorie disponibili per le app che partecipano al programma Per la famiglia:

**Azione e avventura:** app/giochi orientati all'azione che comprendono una grande varietà di contenuti, dai giochi di gare automobilistiche ad avventure fantastiche, ad altre app e giochi progettati per coinvolgere l'utente.

**Giochi di logica:** giochi che stimolano la riflessione, tra cui rompicapo, abbinamenti, quiz e altri giochi che mettono alla prova la memoria, l'intelligenza o la logica.

**Creatività:** app e giochi che stimolano la creatività, tra cui app di disegno o pittura, app di codifica e altre app e giochi di tipo creativo.

**Istruzione:** app e giochi progettati con il contributo di esperti dell'apprendimento (ad esempio, educatori, specialisti dell'apprendimento, ricercatori) per promuovere l'apprendimento, ad esempio accademico, socio-emotivo, fisico e creativo, così come relativo a capacità di base, al pensiero critico e al problem solving.

**Musica e video:** app e giochi con una componente musicale o video, dalle app di simulazione di strumenti a quelle che offrono contenuti video e audio musicali.

**Giochi di ruolo:** app e giochi in cui l'utente può interpretare un ruolo, ad esempio fingendo di essere un cuoco o cuoca, un infermiere o infermiera, un principe o principessa, un vigile o vigilessa del fuoco, un poliziotto o poliziotta o un personaggio immaginario.

---

## 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 relativi al formato

La monetizzazione e la pubblicità nell'app non devono avere contenuti ingannevoli o essere strutturate in modo da determinare clic involontari da parte di bambini o ragazzi. Sono vietati:

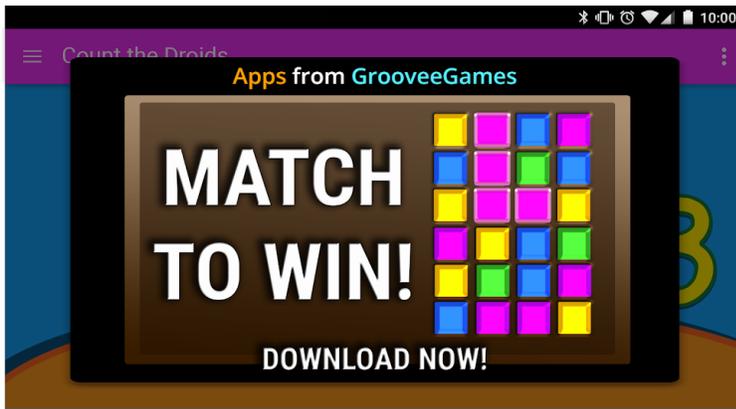
- Monetizzazione e pubblicità improvvisate, incluse la monetizzazione e la pubblicità che occupano l'intero schermo o che interferiscono con il normale utilizzo e non forniscono un modo chiaro per ignorare l'annuncio (ad esempio [ad wall](#)).
- Monetizzazione e pubblicità che interferiscono con il normale gameplay o utilizzo dell'app e che non possono essere chiuse dopo 5 secondi.
- Monetizzazione e pubblicità che non interferiscono con il normale gameplay o utilizzo dell'app possono rimanere visualizzate per più di 5 secondi (ad esempio, contenuti video con annunci integrati).
- Monetizzazione e pubblicità interstitial visualizzate 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).
- Monetizzazione e pubblicità che non sono chiaramente distinguibili dai contenuti dell'app.
- Uso di tattiche emotivamente manipolative o scioccanti per incoraggiare la visualizzazione di annunci o gli acquisti in-app.
- Mancata distinzione tra l'uso di monete virtuali nei giochi rispetto a soldi reali per effettuare acquisti in-app.

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.

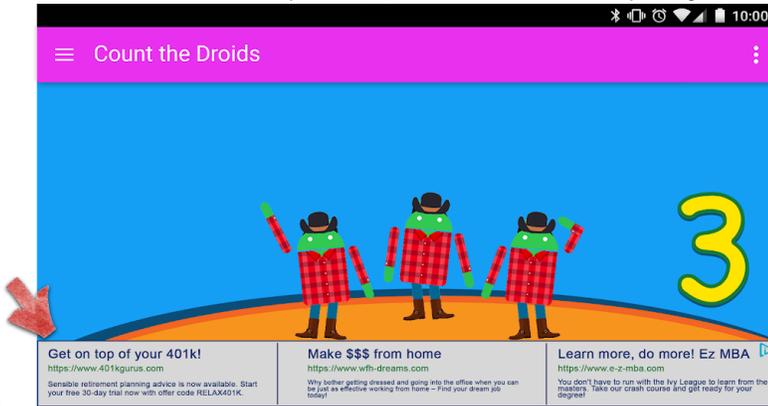
- Monetizzazione e pubblicità che si allontanano dal dito dell'utente mentre questi tenta di chiuderle.
- Monetizzazione e pubblicità che non forniscono all'utente un modo per chiudere l'offerta dopo cinque (5) secondi, come illustrato nell'esempio seguente:



- 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:



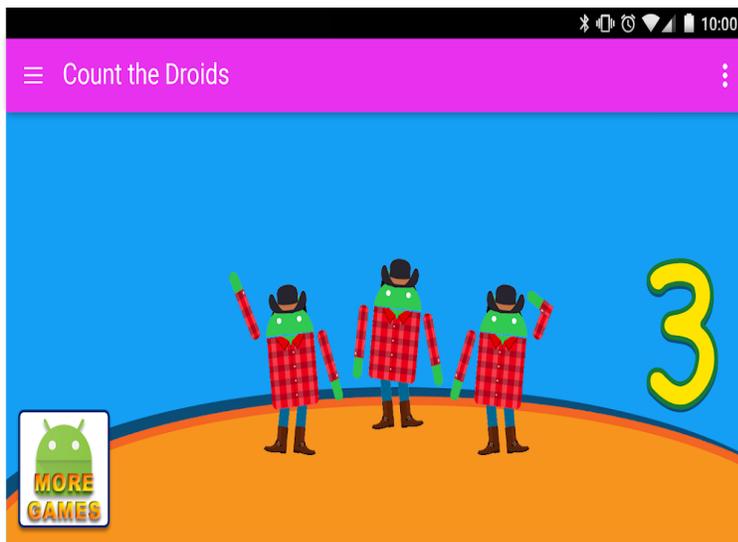
- Annunci banner che mostrano più offerte, come illustrato nell'esempio seguente:



- 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 di annunci

Se pubblichi annunci nella tua app e questa è destinata soltanto un pubblico di minori, devi utilizzare [SDK degli annunci certificati di Google Play](#). Se il pubblico di destinazione dell'app è costituito da bambini e ragazzi e da utenti di età più elevata, devi implementare misure di controllo dell'età, come un [filtro di controllo dell'età](#) e assicurarti che gli annunci mostrati ai bambini provengano esclusivamente dagli SDK di annunci certificati di Google Play. Per le app del programma Per la famiglia è necessario utilizzare soltanto SDK di annunci autocertificati.

Consultare la pagina [Norme del Programma relativo agli annunci per la famiglia](#) per maggiori dettagli su questi requisiti e per consultare l'elenco aggiornato degli SDK di annunci approvati.

Se si utilizza AdMob, fare riferimento al [Centro assistenza AdMob](#) per ulteriori informazioni sui prodotti.

È tua responsabilità garantire che la tua app soddisfi tutti i requisiti relativi a pubblicità, acquisti in-app e contenuti commerciali. Contattare il fornitore o i fornitori degli SDK di annunci per ulteriori informazioni sulle norme relative ai contenuti e sulle prassi pubblicitarie da loro applicate.

#### Acquisti in-app

Per le app che partecipano al programma Per la famiglia, Google Play esegue nuovamente l'autenticazione di tutti gli utenti prima di qualsiasi acquisto in-app. Questa misura serve ad assicurare che gli acquisti vengano effettuati dalla parte finanziariamente responsabile e non da bambini.

---

## Applicazione

Evitare le violazioni delle norme è sempre meglio che doverle gestire ma, qualora si verificano, 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 ti avvisa se un'app viene rimossa dal Google Play Store perché potrebbe accedere alle tue informazioni personali; avrai la possibilità di disinstallare l'app.

---

## Procedura di applicazione

Se la tua app viola una delle nostre norme, prenderemo le misure opportune, come descritto di seguito. Inoltre, ti forniremo via email informazioni pertinenti sull'azione che abbiamo intrapreso, insieme alle istruzioni su come presentare ricorso se ritieni che ci sia stato un errore.

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

Violazioni gravi o ripetute (quali malware, frodi 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 sulla tua app in modi altrettanto differenti. La seguente sezione descrive le varie azioni che Google Play potrebbe intraprendere e il relativo impatto sull'app e/o sul tuo account sviluppatore Google Play. Queste informazioni sono spiegate anche in [questo video](#).

### 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 visualizzare la scheda dello Store, le installazioni, le statistiche e le valutazioni dell'app. 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 reputazione del tuo account sviluppatore Google Play, ma rimozioni multiple potrebbero comportare la sospensione dell'account.

Nota: non tentare di ripubblicare un'app rimossa fino a quando tutte le violazioni delle norme non saranno state risolte.

### 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 è sospesa, gli utenti non potranno visualizzare la scheda dello Store, le installazioni, le statistiche e le valutazioni esistenti dell'app. Queste informazioni verranno ripristinate una volta che avrai inviato un aggiornamento conforme alle norme.
- 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 finché una versione conforme alle norme non verrà approvata da Google Play.
- Le sospensioni incidono, in qualità di avvertimenti, sulla buona reputazione del tuo account sviluppatore Google Play. Più avvertimenti possono comportare la chiusura degli account sviluppatore Google Play individuali e correlati.

Nota: non tentare di ripubblicare un'app sospesa a meno che Google Play non ti abbia indicato che puoi farlo.

### 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 del Play Store dell'app.
- Lo stato di Visibilità limitata dell'app non influisce sulla buona reputazione del tuo account sviluppatore Google Play.
- Lo stato di Visibilità limitata non incide sulla capacità degli utenti di visualizzare la scheda dello Store, le installazioni, le statistiche e le valutazioni dell'app esistenti.

### 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.

## 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 la chiusura del tuo account Play Console.
- Poiché le app all'interno dell'account chiuso vengono rimosse, gli utenti non saranno in grado di visualizzare la scheda dello Store, le installazioni, le statistiche e le valutazioni dell'app esistenti.

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 in base al [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 attività illecite, 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

Ripristineremo le applicazioni se è stato commesso un errore e riscontreremo che la tua 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 stata presa erroneamente, segui le istruzioni fornite nell'email di notifica del provvedimento di applicazione 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

Google Play intende offrire a tutti gli utenti esperienze straordinarie e sicure con le app e a tutti i suoi sviluppatori grandi opportunità per avere successo. Ci impegniamo per garantire la massima fluidità della procedura per rendere disponibile un'app.

Per evitare violazioni comuni che possono rallentare la procedura di revisione o portare a un rifiuto, assicurati di svolgere i passaggi che seguono quando invii informazioni tramite Play Console.

Prima di inviare l'app, devi:

- Fornire in modo accurato tutte le informazioni e i metadati dell'app.
- Verificare che i dati di contatto siano aggiornati.
- 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 per la revisione della tua app (credenziali di accesso, codice QR e così via).

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