

# Kebijakan Program Developer (efektif mulai 1 Oktober 2020)

## Mari membangun sumber aplikasi dan game paling terpercaya di dunia

Inovasi Adalah yang mendorong kesuksesan kita bersama. Namun dengan itu, muncul sebuah tanggung jawab. Kebijakan Program Developer ini, beserta [Perjanjian Distribusi Developer](#), memastikan bahwa, bersama-sama, kita dapat terus menghadirkan aplikasi paling inovatif dan terpercaya di dunia kepada lebih dari satu miliar pengguna melalui Google Play. Kami mengundang Anda untuk mempelajari kebijakan kami di bawah ini.

## Konten yang Dibatasi

Orang-orang dari seluruh dunia menggunakan Google Play untuk mengakses aplikasi dan game setiap harinya. Sebelum mengirimkan aplikasi, pastikan aplikasi Anda sesuai untuk Google Play dan mematuhi hukum setempat.

## Membahayakan Anak

Aplikasi yang berisi konten tentang anak di bawah umur dalam konteks seksual dapat langsung dihapus dari Play Store-, termasuk tetapi tidak terbatas pada, aplikasi yang mendorong perilaku pedofilia atau interaksi tidak pantas yang ditujukan kepada anak di bawah umur (misalnya meraba atau membelai).

Selain itu, aplikasi yang menarik bagi anak-anak tetapi menyertakan tema dewasa juga tidak diizinkan, termasuk tetapi tidak terbatas pada, aplikasi yang memuat unsur kekerasan, darah, dan adegan menyeramkan yang berlebihan; aplikasi yang menggambarkan atau mendorong aktivitas yang membahayakan dan berbahaya. Kami juga tidak mengizinkan aplikasi yang menampilkan gambar bentuk tubuh atau wajah yang negatif, termasuk aplikasi yang menggambarkan operasi plastik, penurunan berat badan, dan penyesuaian kosmetik lainnya terhadap penampilan fisik seseorang untuk tujuan hiburan.

Jika kami mendapati konten berisi gambar pelecehan seksual terhadap anak-anak, kami akan melaporkannya kepada pihak berwajib dan menghapus Akun Google orang-orang yang menyebarkan konten tersebut.

## Konten Tidak Pantas

Untuk memastikan bahwa Google Play tetap menjadi platform yang aman dan sopan, kami telah membuat standar yang mendefinisikan dan melarang konten yang berbahaya atau tidak pantas bagi pengguna kami.

## Konten Seksual dan Bahasa Tidak Sopan

Kami tidak mengizinkan aplikasi yang mengandung atau mempromosikan konten seksual atau bahasa tidak sopan, termasuk pornografi, atau konten atau layanan apa pun yang dimaksudkan untuk memberi kepuasan seksual. Konten yang berisi ketelanjangan dapat diizinkan jika tujuan utamanya adalah untuk edukasi, dokumenter, ilmiah, atau artistik, dan tidak ditampilkan secara mencolok.

Berikut beberapa contoh pelanggaran umum:

- Penggambaran ketelanjangan seksual, atau pose yang menjurus ke arah seksual dengan subjek yang telanjang, diburamkan atau berpakaian minim, dan/atau yang pakaiannya dianggap tidak pantas dalam konteks publik.
- Penggambaran, animasi atau ilustrasi tindakan seksual, pose yang menjurus ke arah seksual, atau penggambaran seksual tentang bagian tubuh.
- Konten yang menggambarkan atau merupakan alat bantu seks, panduan seks, tema seksual ilegal, dan fetisisme.
- Konten vulgar atau tidak sopan, termasuk tetapi tidak terbatas pada, konten yang mungkin memuat bahasa tidak sopan, penghinaan, teks eksplisit, kata kunci dewasa/seksual di listingan Play Store atau dalam aplikasi.
- Konten yang menggambarkan, menjelaskan, atau mendorong bestialitas.
- Aplikasi yang mempromosikan hiburan yang berhubungan dengan seks, layanan escort, atau layanan lain yang dapat dianggap menyediakan aktivitas seksual dengan imbalan.
- Aplikasi yang merendahkan atau menghina orang lain.

## Ujaran Kebencian

Kami tidak mengizinkan aplikasi yang mendorong kekerasan, atau menghasut kebencian terhadap individu atau kelompok berdasarkan ras atau asal etnis, agama, disabilitas, usia, kebangsaan, status veteran, orientasi seksual, gender, identitas gender, atau karakteristik lainnya yang terkait dengan diskriminasi atau marginalisasi yang dilakukan secara sistematis.

Aplikasi dengan konten EDSA (Edukasi, Dokumenter, Ilmiah, atau Artistik) yang terkait dengan Nazi dapat diblokir di negara tertentu, sesuai dengan hukum dan peraturan setempat.

Berikut beberapa contoh pelanggaran umum:

- Konten atau ucapan yang menyatakan bahwa suatu kelompok yang dilindungi tidak berperikemanusiaan, rendahan, atau layak dibenci.
- Aplikasi yang berisi penghinaan, stereotip, atau teori kebencian yang menyebutkan bahwa kelompok yang dilindungi memiliki karakteristik negatif (misalnya berbahaya, korup, jahat, dsb.), atau secara eksplisit atau implisit mengklaim bahwa kelompok tersebut adalah ancaman.
- Konten atau ucapan yang mencoba menghasut orang lain agar percaya bahwa seseorang harus dibenci atau didiskriminasi karena mereka merupakan anggota dari suatu kelompok yang dilindungi.
- Konten yang mempromosikan simbol kebencian, seperti bendera, simbol, lambang, perlengkapan, atau perilaku yang dikaitkan dengan kelompok kebencian.

## Kekerasan

Kami tidak mengizinkan aplikasi yang menggambarkan atau memfasilitasi kekerasan yang tidak beralasan atau aktivitas berbahaya lainnya. Aplikasi yang menggambarkan kekerasan fiksi dalam konteks game, seperti kartun, berburu, atau memancing umumnya diperbolehkan.

Berikut beberapa contoh pelanggaran umum:

- Penggambaran grafis atau deskripsi kekerasan atau ancaman kekerasan yang realistis terhadap orang maupun hewan.
- Aplikasi yang mempromosikan tindakan menyakiti diri sendiri, bunuh diri, perundungan (bullying), pelecehan, penyimpangan pola makan, game mencekik, atau tindakan lain yang dapat mengakibatkan cedera serius atau kematian.

## Konten Teroris

Kami tidak mengizinkan organisasi teroris memublikasikan aplikasi di Google Play untuk tujuan apa pun, termasuk untuk perekrutan.

Kami tidak mengizinkan aplikasi yang kontennya terkait dengan terorisme, seperti konten yang mendukung tindakan teroris, memicu kekerasan, atau merayakan serangan teroris. Jika Anda memposting konten terkait terorisme untuk tujuan edukasi, dokumenter, ilmiah, atau artistik, harap berikan informasi yang cukup agar pengguna dapat memahami konteksnya.

## Peristiwa Sensitif

Kami tidak mengizinkan aplikasi yang tidak memiliki sensitivitas yang wajar terhadap atau memanfaatkan peristiwa bencana alam, kekejaman, konflik, kematian, atau peristiwa tragis lainnya. Aplikasi yang berisi konten terkait peristiwa sensitif umumnya diizinkan apabila memiliki nilai EDSA (Edukasi, Dokumenter, Ilmiah, atau Artistik) atau bertujuan untuk memperingatkan pengguna atau meningkatkan kesadaran terhadap peristiwa sensitif tersebut.

Berikut beberapa contoh pelanggaran umum:

- Kurangnya kepekaan mengenai kasus kematian seseorang atau sekelompok orang karena bunuh diri, overdosis, penyebab alami, dll.
- Tidak mengakui terjadinya peristiwa tragis berskala besar.
- Tampak mencari keuntungan dari peristiwa tragis tanpa manfaat nyata bagi korban.

## Perundungan (Bullying) dan Pelecehan

Kami tidak mengizinkan aplikasi yang berisi atau memfasilitasi ancaman, pelecehan, atau perundungan (bullying).

Berikut beberapa contoh pelanggaran umum:

- Melakukan perundungan (bullying) terhadap korban konflik internasional atau agama.
- Konten yang berupaya mengeksploitasi orang lain, termasuk pemerasan, dll.
- Memposting konten dengan maksud mempermalukan seseorang di depan umum.
- Melecehkan korban peristiwa tragis, atau teman dan keluarganya.

## Produk Berbahaya

Kami tidak mengizinkan aplikasi yang memfasilitasi penjualan bahan peledak, senjata api, amunisi, atau aksesori senjata api tertentu.

- Aksesori yang dibatasi meliputi aksesori yang memungkinkan senjata api untuk mensimulasikan tembakan otomatis atau mengubah senjata api biasa menjadi senjata api otomatis (misalnya bump stock, gatling trigger, drop-in auto sear, kit konversi), dan magasin atau sabuk yang memuat lebih dari 30 peluru.

Kami tidak mengizinkan aplikasi yang memberikan petunjuk pembuatan bahan peledak, senjata api, amunisi, aksesori senjata api yang dibatasi, atau senjata lainnya. Larangan ini mencakup petunjuk tentang mengubah senjata api biasa menjadi senjata api otomatis, atau simulasi kemampuan menembak otomatis.

## Ganja

Kami tidak mengizinkan aplikasi yang memfasilitasi penjualan ganja atau produk ganja, terlepas dari legalitasnya.

Berikut beberapa contoh pelanggaran umum:

- Mengizinkan pengguna memesan ganja melalui fitur keranjang belanja dalam aplikasi.
- Membantu pengguna mengatur pengiriman atau pengambilan ganja.
- Memfasilitasi penjualan produk yang mengandung THC (Tetrahidrokanabinol), termasuk produk seperti minyak CBD yang mengandung THC.

## Tembakau dan Alkohol

Kami tidak mengizinkan aplikasi yang memfasilitasi penjualan tembakau (termasuk rokok elektrik dan stik vape) atau mendorong penggunaan alkohol atau tembakau secara ilegal atau tidak pantas.

Berikut beberapa contoh pelanggaran umum:

- Menggambarkan atau mendorong penggunaan atau penjualan alkohol atau tembakau kepada anak di bawah umur.
- Menyiratkan bahwa mengonsumsi tembakau dapat meningkatkan status sosial, seksual, profesional, intelektual, atau atletis.
- Menggambarkan efek positif meminum minuman beralkohol secara berlebihan, termasuk penggambaran efek positif dari meminum minuman beralkohol secara berlebihan, pesta, atau kompetisi minum minuman keras.

## Jasa Keuangan

Kami tidak mengizinkan aplikasi yang menawarkan produk dan layanan keuangan yang menipu atau berbahaya kepada pengguna.

Untuk tujuan kebijakan ini, kami menganggap produk dan layanan keuangan sebagai produk dan layanan yang terkait dengan pengelolaan atau investasi uang dan mata uang kripto, termasuk saran yang dipersonalisasi.

Jika aplikasi Anda memuat atau mempromosikan produk dan jasa keuangan, Anda harus mematuhi peraturan setempat dan negara bagian di wilayah atau negara mana pun yang ditargetkan oleh aplikasi Anda, misalnya dengan menyertakan pengungkapan tertentu yang disyaratkan oleh hukum setempat.

## Opsi Biner

Kami tidak mengizinkan aplikasi yang memfasilitasi pengguna untuk melakukan perdagangan opsi biner.

## Mata Uang Kripto

Kami tidak mengizinkan aplikasi yang menambang mata uang kripto di perangkat. Kami mengizinkan aplikasi yang mengelola penambangan mata uang kripto dari jarak jauh.

## Pinjaman pribadi

Kami mendefinisikan pinjaman pribadi sebagai peminjaman uang dari perorangan, organisasi, atau entitas kepada konsumen perorangan secara tidak berulang, bukan untuk tujuan membiayai pembelian aset tetap atau edukasi. Konsumen pinjaman pribadi memerlukan informasi tentang kualitas, fitur, biaya, jadwal pelunasan, risiko, dan manfaat produk pinjaman untuk membuat keputusan yang tepat terkait pengambilan pinjaman.

- Contoh: Pinjaman pribadi, kredit tanpa agunan, pinjaman peer-to-peer, pinjaman dengan jaminan BPKB
- Tidak termasuk: Hipotek, kredit kendaraan bermotor, pinjaman pelajar, fasilitas kredit yang bergulir (seperti kartu kredit, fasilitas kredit pribadi)

Aplikasi yang menyediakan pinjaman pribadi, termasuk tetapi tidak terbatas pada, aplikasi yang menawarkan pinjaman secara langsung, perolehan prospek, dan yang menghubungkan konsumen dengan pemberi pinjaman pihak ketiga, harus mengungkapkan informasi berikut dalam metadata aplikasi:

- Periode minimum dan maksimum pelunasan
- Persentase Bunga Tahunan (APR) Maksimum, yang umumnya mencakup suku bunga ditambah biaya dan pengeluaran lainnya selama setahun, atau persentase serupa lainnya yang dihitung secara konsisten dengan hukum setempat
- Contoh representatif jumlah total pinjaman, termasuk semua biaya yang berlaku
- Kebijakan privasi yang secara komprehensif mengungkapkan akses, pengumpulan, penggunaan, dan aktivitas berbagi data pengguna yang bersifat pribadi dan sensitif.

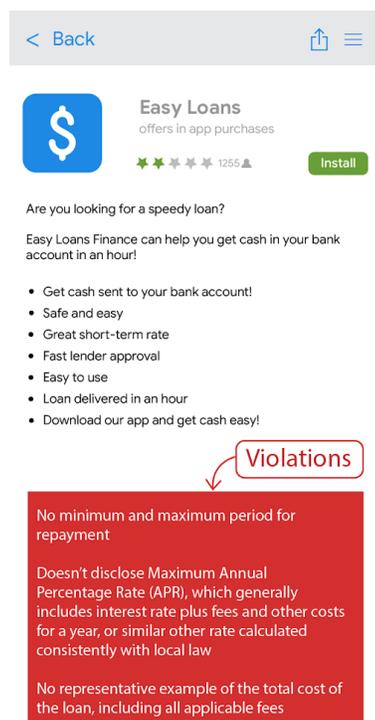
Kami tidak mengizinkan aplikasi yang mempromosikan pinjaman pribadi yang mengharuskan pelunasan penuh dalam waktu 60 hari atau kurang sejak tanggal pinjaman diberikan (kami menyebutnya sebagai "pinjaman pribadi jangka pendek").

#### Pinjaman pribadi dengan Persentase Bunga Tahunan (APR) tinggi

Di Amerika Serikat, kami tidak mengizinkan aplikasi untuk pinjaman pribadi dengan Persentase Bunga Tahunan (APR) sebesar 36% atau lebih. Aplikasi untuk pinjaman pribadi di Amerika Serikat harus menampilkan APR maksimumnya, yang dihitung sesuai dengan [Truth in Lending Act \(TILA\)](#).

Kebijakan ini berlaku untuk aplikasi yang menawarkan pinjaman secara langsung, perolehan prospek, dan yang menghubungkan konsumen dengan pemberi pinjaman pihak ketiga.

Berikut adalah contoh pelanggaran umum:



## Game, Kontes, dan Perjudian dengan Uang

Kami mengizinkan aplikasi perjudian dengan uang, iklan terkait perjudian dengan uang, dan aplikasi olahraga fantasi harian yang memenuhi persyaratan tertentu.

### Aplikasi Perjudian

Kami hanya mengizinkan konten dan layanan yang memfasilitasi perjudian online di:

- Inggris Raya, Irlandia, dan Prancis
- Brasil (terbatas untuk aplikasi yang disetujui yang dipublikasikan oleh Caixa Economica Federal)

Aplikasi ini harus memenuhi persyaratan berikut:

- Developer harus berhasil [menyelesaikan proses pengajuan](#) agar dapat mendistribusikan aplikasi di Google Play;

- Aplikasi harus mematuhi semua hukum dan standar industri yang berlaku untuk setiap negara tempat aplikasi tersebut didistribusikan;
- Developer harus memiliki lisensi perjudian yang valid untuk setiap negara tempat aplikasi tersebut didistribusikan;
- Aplikasi harus mencegah pengguna di bawah umur agar tidak mengakses aplikasi perjudian;
- Aplikasi harus mencegah penggunaan aplikasi di negara yang tidak dilindungi oleh lisensi perjudian yang disediakan developer;
- Aplikasi TIDAK boleh dapat dibeli sebagai aplikasi berbayar di Google Play, maupun menggunakan Penagihan via Google Play;
- Aplikasi harus dapat didownload dan diinstal dari Play Store secara gratis;
- Aplikasi harus memiliki rating AO (Adult Only/Khusus Dewasa) atau setara dengan IARC; dan
- Aplikasi dan listing aplikasinya harus secara jelas menampilkan informasi tentang perjudian yang bertanggung jawab.

Untuk semua lokasi lainnya, kami tidak mengizinkan konten atau layanan yang memfasilitasi perjudian online, termasuk, tetapi tidak terbatas pada, kasino online, taruhan olahraga dan lotre, serta permainan keterampilan yang menawarkan hadiah uang tunai atau nilai lainnya.

## Aplikasi Turnamen, Kontes, dan Game dengan Uang Lainnya

Kami melarang konten atau layanan yang memungkinkan atau memfasilitasi kemampuan pengguna untuk bertaruh, mempertaruhkan, atau berpartisipasi menggunakan uang sungguhan (termasuk item dalam aplikasi yang dibeli dengan uang) untuk mendapatkan hadiah bernilai uang sungguhan. Ini termasuk, tetapi tidak terbatas pada, kasino online, taruhan olahraga, lotre yang gagal memenuhi persyaratan aplikasi Perjudian yang disebutkan di atas, dan game yang menawarkan hadiah uang tunai atau yang bernilai sungguhan lainnya.

Berikut beberapa contoh pelanggaran:

- Game yang menerima uang dengan memberi kesempatan memenangkan hadiah fisik atau uang sebagai imbalannya
- Game dengan poin "loyalitas" (misalnya interaksi atau aktivitas) yang (1) dapat ditambah atau dipercepat melalui pembelian dengan uang sungguhan yang (2) dapat ditukarkan dengan item atau hadiah bernilai uang sungguhan
- Aplikasi yang menerima atau mengelola taruhan perjudian, mata uang dalam aplikasi yang diperlukan untuk partisipasi, kemenangan, atau setoran guna mendapatkan atau mempercepat kelayakan untuk mendapatkan hadiah fisik atau uang.
- Aplikasi yang menyertakan "pesan ajakan" untuk bertaruh, mempertaruhkan, atau berpartisipasi dalam permainan, kontes, atau turnamen menggunakan uang sungguhan, seperti aplikasi dengan elemen navigasi (item menu, tab, tombol, dsb.) yang mengundang pengguna untuk memilih "DAFTAR" atau "IKUTI" turnamen agar berkesempatan memenangkan hadiah uang tunai.

## Iklan Perjudian atau Game, Kontes, dan Turnamen dengan Uang dalam Aplikasi yang Didistribusikan oleh Google Play

Kami akan mengizinkan aplikasi yang mengiklankan perjudian atau game, kontes, dan turnamen dengan uang jika memenuhi persyaratan berikut:

- Aplikasi dan iklan (termasuk pengiklan) harus mematuhi semua hukum dan standar industri yang berlaku di lokasi mana pun iklan ditayangkan;
- Iklan harus memenuhi persyaratan lisensi setempat untuk semua produk dan layanan terkait perjudian yang dipromosikan;
- Aplikasi tidak boleh menayangkan iklan perjudian untuk individu berusia di bawah 18 tahun;
- Aplikasi tidak boleh didaftarkan dalam program Didesain untuk Keluarga;
- Aplikasi tidak boleh menargetkan individu berusia di bawah 18 tahun;
- Jika mengiklankan Aplikasi Perjudian (sebagaimana didefinisikan di atas), iklan harus dengan jelas menampilkan informasi tentang perjudian yang bertanggung jawab di halaman landing aplikasi, di listing aplikasi yang diiklankan, atau dalam aplikasi;-
- Aplikasi tidak boleh menyediakan konten simulasi perjudian (misalnya aplikasi kasino sosial; aplikasi dengan mesin slot virtual);
- Aplikasi tidak boleh menyediakan fungsi dukungan untuk perjudian atau game, lotre, atau turnamen yang menggunakan uang sungguhan (misalnya fungsi yang membantu taruhan, pembayaran, pelacakan skor/pejuang pertandingan olahraga, atau pengelolaan dana partisipasi);
- Anda tidak boleh memiliki kepentingan kepemilikan atas layanan perjudian atau game, lotre, atau turnamen dengan uang yang diiklankan dalam aplikasi;
- Konten aplikasi tidak boleh mempromosikan atau mengarahkan pengguna ke layanan perjudian atau game, lotre, atau turnamen dengan uang

Hanya aplikasi Perjudian (sebagaimana didefinisikan di atas) atau aplikasi yang memenuhi semua persyaratan Iklan Perjudian ini yang dapat menyertakan iklan untuk perjudian dengan uang atau game, lotre, maupun turnamen dengan uang.

Berikut beberapa contoh pelanggaran:

- Aplikasi yang didesain untuk pengguna di bawah umur dan menayangkan iklan yang mempromosikan layanan perjudian
- Game simulasi kasino yang mempromosikan atau mengarahkan pengguna ke kasino dengan uang sungguhan
- Aplikasi pelacak peluang pertandingan olahraga khusus yang berisi iklan perjudian terintegrasi yang ditautkan ke situs judi olahraga
- Aplikasi berita yang menayangkan iklan untuk layanan perjudian yang dimiliki atau dioperasikan oleh developer aplikasi
- Aplikasi yang memuat iklan perjudian yang melanggar kebijakan [Iklan yang Menipu](#), seperti iklan yang ditampilkan kepada pengguna sebagai tombol, ikon, atau elemen interaktif lainnya dalam aplikasi

## Aplikasi Olahraga Fantasi Harian (DFS)

Kami hanya mengizinkan aplikasi olahraga fantasi harian (DFS), sebagaimana didefinisikan oleh hukum setempat yang berlaku, jika memenuhi persyaratan berikut:

- Aplikasi 1)-hanya didistribusikan di Amerika Serikat atau 2) memenuhi syarat berdasarkan persyaratan Aplikasi Perjudian yang disebutkan di atas;
- Developer harus berhasil menyelesaikan proses [pengajuan DFS](#) hingga disetujui agar dapat mendistribusikan aplikasi tersebut di Google Play;
- Aplikasi harus mematuhi semua hukum dan standar industri yang berlaku untuk negara tempat aplikasi tersebut didistribusikan;
- Aplikasi harus mencegah pengguna di bawah umur melakukan taruhan atau transaksi keuangan dalam aplikasi;
- Aplikasi TIDAK boleh dapat dibeli sebagai aplikasi berbayar di Google Play, maupun menggunakan Penagihan via Google Play;
- Aplikasi harus dapat didownload dan diinstal dari Play Store secara gratis;
- Aplikasi harus memiliki rating AO (Adult Only/Khusus Dewasa) atau setara dengan IARC; dan
- Aplikasi dan listing aplikasinya harus secara jelas menampilkan informasi tentang perjudian yang bertanggung jawab.

Jika didistribusikan di Amerika Serikat, persyaratan tambahan berikut akan diberlakukan;

- Aplikasi harus mematuhi semua hukum dan standar industri yang berlaku untuk negara bagian AS atau wilayah AS mana pun tempat aplikasi tersebut didistribusikan;
- Developer harus memiliki lisensi yang valid untuk setiap negara bagian AS atau wilayah AS yang mewajibkan lisensi untuk aplikasi olahraga fantasi harian;
- Aplikasi harus melarang penggunaan dari Negara Bagian AS atau wilayah AS tempat developer tidak memiliki lisensi yang diperlukan untuk aplikasi olahraga fantasi harian; dan
- Aplikasi harus melarang penggunaan dari Negara Bagian AS atau wilayah AS yang tidak melegalkan aplikasi olahraga fantasi harian.

## Aktivitas Ilegal

Kami tidak mengizinkan aplikasi yang memfasilitasi atau mempromosikan aktivitas ilegal.

Berikut beberapa contoh pelanggaran umum:

- Memfasilitasi penjualan atau pembelian obat-obatan terlarang atau obat resep tanpa resep dokter.
- Menggambarkan atau mendorong penggunaan atau penjualan obat-obatan, alkohol, atau tembakau oleh anak di bawah umur.
- Menyertakan petunjuk untuk menumbuhkan atau memproduksi obat-obatan terlarang.

## Konten Buatan Pengguna

Konten buatan pengguna (UGC) adalah konten aplikasi yang dikontribusikan oleh pengguna, dan yang dapat dilihat atau diakses oleh setidaknya sebagian kecil pengguna aplikasi tersebut.

Aplikasi yang berisi atau menampilkan UGC harus:

- mewajibkan pengguna menyetujui persyaratan penggunaan dan/atau kebijakan pengguna aplikasi sebelum dapat membuat atau mengupload UGC;

- mendefinisikan konten dan perilaku yang tidak pantas (dengan mematuhi Kebijakan Program Developer Play), dan melarangnya dalam persyaratan penggunaan atau kebijakan pengguna aplikasi;
- mengimplementasikan moderasi UGC yang ketat, efektif, dan berkelanjutan, secara wajar dan sesuai dengan jenis UGC yang dihosting oleh aplikasi
  - Untuk aplikasi live streaming, UGC yang tidak pantas harus dihapus sesegera mungkin;
  - Untuk aplikasi augmented reality (AR), moderasi UGC (termasuk sistem pelaporan dalam aplikasi) harus memperhitungkan UGC AR yang tidak pantas (misalnya gambar AR seksual vulgar) dan lokasi penautan AR yang sensitif (misalnya konten AR yang ditautkan ke area terlarang, seperti markas militer, atau properti pribadi tempat penautan AR dapat menimbulkan masalah bagi pemilik properti);
- menyediakan sistem dalam aplikasi yang mudah digunakan untuk melaporkan UGC yang tidak pantas dan mengambil tindakan terhadap UGC tersebut jika perlu;
- menghapus atau memblokir pengguna yang melakukan pelecehan yang melanggar persyaratan penggunaan dan/atau kebijakan pengguna aplikasi;
- memberikan perlindungan untuk mencegah monetisasi dalam aplikasi agar tidak mendorong perilaku pengguna yang tidak menyenangkan.

Aplikasi yang memiliki tujuan utama untuk menampilkan UGC yang tidak pantas akan dihapus dari Google Play. Demikian pula, aplikasi yang pada akhirnya digunakan terutama untuk menghosting UGC yang tidak pantas, atau mendapatkan reputasi di antara penggunanya karena menjadi tempat berkembangnya konten semacam itu, juga akan dihapus dari Google Play.

Berikut beberapa contoh pelanggaran umum:

- Mempromosikan konten seksual vulgar buatan pengguna, termasuk mengimplementasikan atau mengizinkan fitur berbayar yang utamanya mendorong aktivitas berbagi konten yang tidak pantas.
- Aplikasi berisi konten buatan pengguna (UGC) yang tidak disertai perlindungan memadai terhadap ancaman, pelecehan, atau perundungan (bullying), terutama terhadap anak di bawah umur.
- Postingan, komentar, atau foto dalam aplikasi yang terutama ditujukan untuk melecehkan atau menunjuk seseorang agar jadi sasaran tindak kekerasan, serangan berbahaya, atau bahan ejekan.
- Aplikasi yang terus-menerus gagal mengatasi keluhan pengguna tentang konten yang tidak pantas.

## Zat yang Belum Disetujui

Google Play tidak mengizinkan aplikasi yang mempromosikan atau menjual zat yang belum disetujui, terlepas dari klaim legalitas apa pun. Contoh:

- Semua item dalam daftar [obat dan suplemen terlarang](#) yang tidak lengkap ini
- Produk yang mengandung efedra
- Produk yang mengandung hCG (human chorionic gonadotropin) yang terkait dengan penurunan atau pengendalian berat badan, atau bila dipromosikan bersama steroid anabolik
- Suplemen herbal dan diet dengan bahan obat aktif atau berbahaya
- Klaim kesehatan palsu atau menyesatkan, termasuk klaim yang menyiratkan bahwa produk tertentu sama efektifnya dengan obat resep atau zat terkontrol
- Produk yang disetujui oleh pihak selain pemerintah yang dipasarkan dengan cara sedemikian rupa sehingga menyiratkan bahwa produk tersebut aman atau efektif untuk digunakan dalam mencegah, menyembuhkan, atau mengobati penyakit atau gejala tertentu
- Produk yang telah ditindak atau diperingatkan oleh pemerintah atau badan pengatur
- Produk dengan nama membingungkan yang mirip dengan obat atau suplemen atau zat terkontrol yang tidak disetujui

Untuk mendapatkan informasi tambahan tentang obat-obatan dan suplemen yang tidak disetujui atau menyesatkan yang masuk dalam pantauan kami, kunjungi [www.legitscript.com](http://www.legitscript.com).

## Kekayaan Intelektual

Pemilik karya dapat dirugikan apabila developer menyalin karya orang lain atau menggunakannya tanpa izin yang diperlukan. Jangan pernah menggunakan karya orang lain secara tidak wajar.

### Kekayaan Intelektual

Kami tidak mengizinkan akun developer atau aplikasi yang melanggar hak kekayaan intelektual orang lain (termasuk merek dagang, hak cipta, paten, rahasia dagang, dan kepemilikan lainnya). Kami juga tidak mengizinkan aplikasi yang mendorong atau menyebabkan pelanggaran hak atas kekayaan intelektual.

Kami akan merespons laporan dugaan pelanggaran hak cipta yang jelas. Untuk mengetahui informasi selengkapnya atau untuk mengajukan permintaan DMCA, baca [prosedur hak cipta](#) kami.

Untuk menyampaikan keluhan terkait penjualan atau promosi penjualan barang palsu dalam aplikasi, kirim [pemberitahuan pemalsuan](#).

Jika Anda adalah pemilik merek dagang dan yakin bahwa ada aplikasi di Google Play yang melanggar hak merek dagang Anda, hubungi developer secara langsung untuk menyampaikan kekhawatiran Anda. Jika tidak dapat menemukan penyelesaian masalah dengan developer, sampaikan keluhan merek dagang Anda melalui [formulir](#) ini.

Jika memiliki dokumentasi tertulis yang membuktikan bahwa Anda memiliki izin untuk menggunakan kekayaan intelektual pihak ketiga dalam aplikasi atau listingan Play Store (seperti nama, logo, dan aset visual merek), [hubungi tim Google Play](#) sebelum pengiriman agar aplikasi tidak ditolak karena pelanggaran kekayaan intelektual.

## Penggunaan yang Tidak Sah atas Konten Berhak Cipta

Kami tidak mengizinkan aplikasi yang melanggar hak cipta. Memodifikasi konten berhak cipta masih dapat menyebabkan pelanggaran. Developer mungkin perlu memberikan bukti atas hak mereka untuk menggunakan konten berhak cipta.

Harap berhati-hati saat menggunakan konten berhak cipta untuk menunjukkan fungsi aplikasi Anda. Secara umum, pendekatan yang paling aman adalah dengan membuat konten asli.

Berikut beberapa contoh konten berhak cipta yang sering kali digunakan tanpa izin atau alasan yang sah secara hukum:

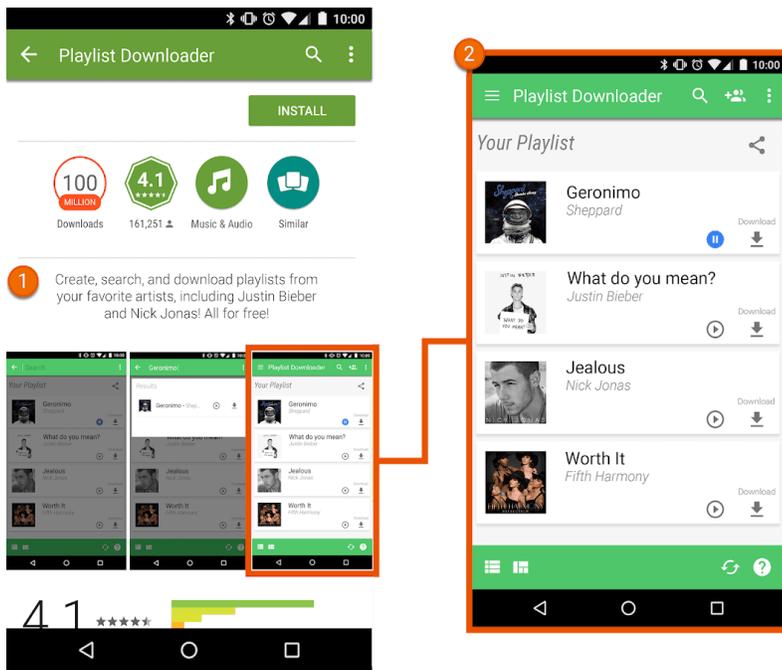
- Gambar sampul untuk album musik, game video, dan buku.
- Gambar pemasaran dari film, televisi, atau video game.
- Visual atau gambar dari buku komik, kartun, film, video musik, atau televisi.
- Logo tim olahraga profesional atau sekolah.
- Foto yang diambil dari akun media sosial tokoh terkenal.
- Gambar profesional dari tokoh terkenal.
- Reproduksi atau "gambar buatan penggemar" (fan art) yang tidak dapat dibedakan dari karya asli berhak cipta.
- Aplikasi yang memutar klip audio dari konten berhak cipta.
- Reproduksi sepenuhnya atau terjemahan dari buku yang tidak dalam domain publik.

## Mendorong Pelanggaran Hak Cipta

Kami tidak mengizinkan aplikasi yang menyebabkan atau mendorong pelanggaran hak cipta. Sebelum memublikasikan aplikasi, periksa apakah ada elemen dalam aplikasi Anda yang mungkin mendorong pelanggaran hak cipta, lalu dapatkan saran hukum jika perlu.

Berikut beberapa contoh pelanggaran umum:

- Aplikasi streaming yang memungkinkan pengguna mendownload salinan lokal konten berhak cipta tanpa izin.
- Aplikasi yang mendorong pengguna untuk melakukan streaming dan mendownload karya berhak cipta, termasuk musik dan video, yang melanggar undang-undang hak cipta yang berlaku:



- ① Deskripsi dalam listing aplikasi ini mendorong pengguna untuk mendownload konten berhak cipta tanpa izin.
- ② Screenshot dalam listing aplikasi ini mendorong pengguna untuk mendownload konten berhak cipta tanpa izin.

## Pelanggaran Merek Dagang

Kami tidak mengizinkan aplikasi yang melanggar merek dagang orang lain. Merek dagang adalah kata, simbol, atau kombinasi yang mengidentifikasi sumber barang atau layanan. Setelah diakuisisi, merek dagang memberikan hak eksklusif kepada pemilik untuk menggunakan merek dagang sehubungan dengan barang atau layanan tertentu.

Pelanggaran merek dagang adalah penggunaan yang tidak benar atau tidak sah dari merek dagang yang identik atau mirip, dengan cara yang cenderung menyebabkan kebingungan atas sumber produk tersebut. Jika aplikasi menggunakan merek dagang pihak lain dengan cara yang kemungkinan akan menyebabkan kebingungan, aplikasi Anda dapat ditangguhkan.

## Pemalsuan

Kami tidak mengizinkan aplikasi yang menjual atau mempromosikan penjualan barang palsu. Barang palsu memiliki merek dagang atau logo yang identik atau sangat sulit dibedakan dari merek aslinya. Barang semacam ini meniru fitur merek produk agar dapat disamakan sebagai produk asli pemilik merek tersebut.

## Privasi, Penipuan, dan Penyalahgunaan Perangkat

Kami berkomitmen untuk melindungi privasi pengguna dan memberikan lingkungan yang aman dan terjamin bagi pengguna. Oleh sebab itu, kami melarang keras aplikasi yang menipu, berbahaya, atau dimaksudkan untuk menyalahgunakan jaringan, perangkat, atau data pribadi apa pun.

## Data Pengguna

Anda harus bersikap transparan mengenai cara Anda menangani data pengguna (misalnya informasi yang dikumpulkan dari atau tentang pengguna, termasuk informasi perangkat). Hal ini berarti mengungkapkan akses, pengumpulan, penggunaan, dan berbagi data oleh aplikasi Anda, serta membatasi penggunaan data untuk tujuan yang diungkapkan. Selain itu, jika aplikasi Anda menangani data pengguna yang bersifat pribadi atau sensitif, lihat persyaratan tambahan pada bagian "Informasi Pribadi dan Sensitif" di bawah ini. Persyaratan Google Play ini merupakan tambahan untuk setiap persyaratan yang ditentukan oleh hukum perlindungan data dan privasi yang berlaku.

## Informasi Pribadi dan Sensitif

Data pengguna yang bersifat pribadi dan sensitif termasuk, tetapi tidak terbatas pada, informasi identitas pribadi, informasi keuangan dan pembayaran, informasi autentikasi, buku telepon, kontak, lokasi perangkat, data panggilan dan SMS, data mikrofon, kamera, dan data penggunaan atau data perangkat sensitif lainnya. Jika aplikasi Anda menangani data pengguna yang sensitif, Anda harus:

- Membatasi akses, pengumpulan, penggunaan, dan berbagi yang Anda lakukan atas data pribadi atau sensitif yang diperoleh melalui aplikasi untuk tujuan yang terkait secara langsung dengan penyediaan dan penyempurnaan fitur aplikasi (misalnya fungsi yang diharapkan pengguna yang didokumentasikan dan dipromosikan dalam deskripsi aplikasi di Play Store). Aplikasi yang memperluas penggunaan data ini untuk menayangkan iklan harus mematuhi [Kebijakan Iklan](#) kami.
- Memposting kebijakan privasi di kolom yang telah ditetapkan di Konsol Play dan dalam aplikasi itu sendiri. Kebijakan privasi, beserta pengungkapan apa pun dalam aplikasi, harus secara komprehensif mengungkapkan cara aplikasi Anda mengakses, mengumpulkan, menggunakan, dan membagikan data pengguna. Kebijakan privasi Anda harus mengungkapkan jenis data pribadi dan sensitif yang diakses, dikumpulkan, digunakan, dan dibagikan aplikasi Anda, dan pihak seperti apa yang Anda ajak bekerja sama untuk berbagi data pengguna yang bersifat sensitif.
- Menangani semua data pengguna yang bersifat pribadi atau sensitif dengan aman, termasuk mentransmisikan melalui kriptografi modern (misalnya, melalui HTTPS).
- Menggunakan permintaan izin waktu proses kapan pun saat tersedia, sebelum mengakses data yang dilindungi oleh [izin Android](#).
- Tidak menjual data pengguna yang bersifat pribadi atau sensitif.

## Pengungkapan yang Jelas dan Persyaratan Izin

Apabila pengguna mungkin tidak mengetahui secara wajar bahwa data pengguna yang bersifat pribadi atau sensitif milik mereka akan diperlukan untuk menyediakan atau menyempurnakan fitur atau fungsi yang mematuhi kebijakan dalam aplikasi Anda (misalnya pengumpulan data yang terjadi di latar belakang aplikasi), Anda harus memenuhi persyaratan berikut:

**Anda harus menyediakan pengungkapan dalam aplikasi terkait akses, pengumpulan, penggunaan, dan aktivitas berbagi data oleh Anda. Pengungkapan dalam aplikasi:**

- Harus ada di dalam aplikasi itu sendiri, tidak hanya dalam deskripsi aplikasi atau di situs;
- Harus ditampilkan dalam penggunaan aplikasi yang normal serta tidak mengharuskan pengguna untuk membuka menu atau setelan;
- Harus menjelaskan data yang sedang diakses atau dikumpulkan;
- Harus menjelaskan cara data akan digunakan dan/atau dibagikan;
- **Tidak boleh** hanya disertakan dalam kebijakan privasi atau persyaratan layanan; dan
- **Tidak boleh** disertakan dengan pengungkapan lain yang tidak terkait dengan pengumpulan data pribadi atau sensitif.

**Pengungkapan dalam aplikasi Anda harus disertakan dengan dan berada tepat sebelum permintaan izin pengguna, dan jika memungkinkan, izin waktu proses yang terkait. Anda tidak boleh mengakses atau mengumpulkan data pribadi atau sensitif apa pun hingga pengguna mengizinkan. Permintaan izin aplikasi:**

- Harus menampilkan dialog izin yang jelas dan tidak ambigu;
- Harus meminta tindakan afirmatif dari pengguna (misalnya mengetuk untuk menyetujui, mencentang kotak centang);
- **Tidak boleh** menginterpretasikan pilihan untuk menutup pengungkapan (termasuk mengetuk untuk menutup atau menekan tombol kembali atau tombol layar utama) sebagai pemberian izin; dan
- **Tidak boleh** menggunakan pesan yang ditutup atau berakhir secara otomatis sebagai cara mendapatkan izin pengguna.

**Berikut beberapa contoh pelanggaran umum:**

- Aplikasi yang mengakses inventaris aplikasi terinstal milik pengguna dan tidak memperlakukan data ini sebagai data pribadi atau sensitif berdasarkan Kebijakan Privasi, penanganan data, serta persyaratan Izin dan Pengungkapan yang Jelas di atas.
- Aplikasi yang mengakses data buku telepon atau kontak pengguna dan tidak memperlakukan data ini sebagai data pribadi atau sensitif berdasarkan Kebijakan Privasi, penanganan data, serta persyaratan izin dan Pengungkapan yang Jelas di atas.
- Aplikasi yang merekam layar pengguna dan tidak memperlakukan data tersebut sebagai data pribadi atau sensitif berdasarkan kebijakan ini.
- Aplikasi yang mengumpulkan [lokasi perangkat](#) dan tidak mengungkapkan penggunaannya secara komprehensif serta memperoleh izin sesuai dengan persyaratan di atas
- Aplikasi yang mengumpulkan izin terbatas di latar belakang aplikasi, termasuk untuk tujuan pelacakan, penelitian, atau pemasaran, tanpa mengungkapkan penggunaannya secara komprehensif dan memperoleh persetujuan sesuai dengan persyaratan di atas.

## Pembatasan Khusus untuk Akses Data Sensitif

Selain persyaratan di atas, tabel di bawah juga menjelaskan persyaratan untuk aktivitas tertentu.

Aktivitas	Persyaratan
Aplikasi Anda menangani informasi pembayaran atau keuangan, atau nomor identitas yang diterbitkan oleh pemerintah	Aplikasi tidak boleh mengungkapkan data pengguna apa pun yang sensitif atau bersifat pribadi, yang berkaitan dengan aktivitas pembayaran atau keuangan maupun nomor identitas yang diterbitkan oleh pemerintah.
Aplikasi Anda menangani informasi kontak atau buku telepon non-publik	Kami tidak mengizinkan penerbitan atau pengungkapan kontak non-publik orang lain secara tidak sah.
Aplikasi Anda menyertakan fungsi keamanan atau antivirus, seperti antivirus, anti-malware, atau fitur terkait keamanan	Aplikasi harus memposting kebijakan privasi, beserta pengungkapan dalam aplikasi, yang menjelaskan data pengguna yang dikumpulkan dan ditransmisikan oleh aplikasi Anda, penggunaannya, dan dengan siapa data tersebut akan dibagikan.

## EU-U.S. Privacy Shield (Perlindungan Privasi EU-AS)

### Perlindungan Privasi

Jika Anda mengakses, menggunakan, atau memproses informasi pribadi yang disediakan oleh Google, yang secara langsung maupun tidak langsung mengidentifikasi pengguna, dan berasal dari Uni Eropa atau Swiss ("Informasi Pribadi Uni Eropa"), Anda harus:

- mematuhi semua hukum privasi, keamanan data, dan perlindungan data, serta instruksi, regulasi, dan peraturan yang berlaku;
- mengakses, menggunakan, atau memproses Informasi Pribadi Uni Eropa hanya untuk tujuan yang sesuai dengan persetujuan yang didapatkan dari pengguna yang berkaitan dengan Informasi Pribadi Uni Eropa tersebut;
- mengimplementasikan langkah-langkah teknis dan organisasional yang sesuai untuk melindungi Informasi Pribadi Uni Eropa dari kehilangan, penyalahgunaan, serta akses, pengungkapan, perubahan, dan perusakan yang tidak sah atau melanggar hukum; dan
- memberikan level perlindungan yang sama seperti yang diwajibkan oleh [Prinsip Privacy Shield \(Perlindungan Privasi\)](#).

Anda harus memantau kepatuhan Anda terhadap ketentuan tersebut secara berkala. Jika sewaktu-waktu Anda tidak dapat memenuhi ketentuan ini (atau jika ada risiko signifikan sehingga Anda tidak dapat memenuhinya), Anda harus segera memberi tahu kami melalui email ke [data-protection-office@google.com](mailto:data-protection-office@google.com) dan segera menghentikan pemrosesan Informasi Pribadi EU atau melakukan langkah-langkah yang wajar dan sesuai untuk mengembalikan perlindungan ke level yang memadai.

## Izin

Permintaan izin harus dapat dipahami oleh pengguna. Anda hanya boleh meminta izin yang diperlukan untuk menerapkan fitur atau layanan saat ini di aplikasi Anda yang dipromosikan dalam listingan Play Store Anda. Anda tidak boleh menggunakan izin yang memberikan akses ke data pengguna atau data perangkat untuk fitur atau tujuan yang tidak diungkapkan, tidak diterapkan, atau tidak diizinkan. Data pribadi atau sensitif yang diakses melalui izin sama sekali tidak boleh dijual.

Meminta izin untuk mengakses data sesuai konteks (melalui autentikasi tambahan), sehingga pengguna memahami alasan aplikasi Anda memerlukan izin tersebut. Gunakan data hanya untuk tujuan yang diizinkan oleh pengguna. Jika nantinya Anda ingin menggunakan data tersebut untuk tujuan lain, Anda harus bertanya kepada pengguna dan memastikan pengguna menyetujui penggunaan tambahan tersebut.

### Izin Terbatas

Selain hal di atas, izin terbatas adalah izin yang ditetapkan sebagai [Berbahaya](#), [Khusus](#), atau [Tanda Tangan](#), dan tunduk pada persyaratan dan pembatasan tambahan berikut:

- Data pengguna atau data perangkat sensitif yang diakses melalui Izin Terbatas hanya boleh ditransfer ke pihak ketiga jika diperlukan untuk menyediakan atau menyempurnakan fitur atau layanan saat ini dalam aplikasi yang menjadi sumber pengumpulan data. Anda juga boleh mentransfer data sebagaimana yang diperlukan untuk mematuhi undang-undang yang berlaku atau sebagai bagian dari merger, akuisisi, atau penjualan aset dengan pemberitahuan yang memadai secara hukum kepada pengguna. Semua transfer atau penjualan data pengguna lainnya tidak diperbolehkan.
- Hormati keputusan pengguna jika mereka menolak permintaan untuk Izin Terbatas, dan pengguna tidak boleh dimanipulasi atau dipaksa untuk menyetujui izin yang tidak benar-benar diperlukan. Anda harus melakukan upaya yang

wajar untuk memfasilitasi pengguna yang tidak memberikan akses ke izin sensitif (misalnya memungkinkan pengguna memasukkan nomor telepon secara manual jika mereka membatasi akses ke Log Panggilan).

Izin Terbatas tertentu dapat tunduk pada persyaratan lainnya seperti yang dijelaskan di bawah. Tujuan batasan ini adalah untuk mengamankan privasi pengguna. Kami dapat membuat pengecualian terbatas pada persyaratan di bawah ini dalam situasi yang sangat jarang terjadi jika aplikasi menyediakan fitur yang sangat menarik atau penting dan jika tidak ada metode alternatif yang tersedia untuk menyajikan fitur tersebut. Kami mengevaluasi pengecualian yang diajukan terhadap potensi dampak privasi atau keamanan pada pengguna.

## Izin SMS dan Log Panggilan

Izin SMS dan Log Panggilan dianggap sebagai data pengguna yang bersifat pribadi dan sensitif berdasarkan kebijakan [Informasi Pribadi dan Sensitif](#), serta pembatasan berikut:

Izin Terbatas	Persyaratan
Manifes aplikasi Anda meminta grup izin Log Panggilan (misalnya READ_CALL_LOG, WRITE_CALL_LOG, PROCESS_OUTGOING_CALLS)	Izin harus terdaftar secara aktif sebagai pengendali Telepon atau Asisten default di perangkat.
Manifes aplikasi Anda meminta grup izin SMS (misalnya READ_SMS, SEND_SMS, WRITE_SMS, RECEIVE_SMS, RECEIVE_WAP_PUSH, RECEIVE_MMS)	Izin harus terdaftar secara aktif sebagai pengendali SMS atau Asisten default di perangkat.

Aplikasi yang tidak memiliki kemampuan menjadi pengendali SMS, Telepon, atau Asisten default tidak boleh menyatakan penggunaan izin di atas dalam manifesnya. Hal ini mencakup teks placeholder dalam manifes. Selain itu, aplikasi harus terdaftar secara aktif sebagai pengendali SMS, Telepon, atau Asisten default sebelum meminta pengguna menyetujui salah satu izin di atas dan harus segera berhenti menggunakan izin tersebut ketika tidak lagi menjadi pengendali default. Penggunaan dan pengecualian yang diizinkan tersedia di [halaman Pusat Bantuan ini](#).

Aplikasi hanya boleh menggunakan izin (dan data apa pun yang dihasilkan dari izin tersebut) untuk menyediakan fungsi aplikasi inti yang disetujui. Fungsi inti didefinisikan sebagai tujuan utama aplikasi, yang mungkin meliputi serangkaian fitur inti, yang semuanya harus didokumentasikan dan ditampilkan dengan jelas dalam deskripsi aplikasi. Tanpa fitur inti, aplikasi akan dianggap "rusak" atau tidak dapat digunakan. Transfer, berbagi, atau penggunaan berlisensi atas data ini hanya diperbolehkan untuk menyediakan fitur atau layanan inti dalam aplikasi, dan penggunaannya tidak boleh diperluas untuk tujuan lain (misalnya untuk menyempurnakan aplikasi atau layanan lain, periklanan, atau pemasaran). Anda tidak boleh menggunakan metode alternatif (termasuk sumber pihak ketiga, API, atau izin lain) untuk mendapatkan data yang diatribusikan dengan izin terkait Log Panggilan atau SMS.

## Izin Akses Lokasi

[Lokasi perangkat](#) dianggap sebagai data pengguna yang bersifat pribadi dan sensitif berdasarkan kebijakan [Informasi Pribadi dan Sensitif](#), serta persyaratan berikut:

- Aplikasi tidak boleh mengakses data yang dilindungi oleh izin akses lokasi (misalnya ACCESS\_FINE\_LOCATION, ACCESS\_COARSE\_LOCATION, ACCESS\_BACKGROUND\_LOCATION) setelah data tidak lagi diperlukan untuk menyampaikan fitur atau layanan saat ini di aplikasi Anda.
- Anda tidak boleh meminta izin akses lokasi dari pengguna semata-mata untuk tujuan iklan atau analisis. Aplikasi yang memperluas penggunaan yang diizinkan atas data ini untuk menayangkan iklan harus mematuhi [Kebijakan Iklan](#) kami.
- Aplikasi harus meminta cakupan minimum yang diperlukan (yaitu sementara, bukan terperinci, dan latar depan, bukan latar belakang) untuk menyediakan fitur atau layanan saat ini yang memerlukan lokasi, dan pengguna harus mengetahui secara wajar bahwa fitur atau layanan tersebut memerlukan level lokasi yang diminta. Sebagai contoh, kami dapat menolak aplikasi yang meminta atau mengakses lokasi latar belakang tanpa alasan yang meyakinkan.
- Lokasi latar belakang hanya dapat digunakan untuk menyediakan fitur yang bermanfaat bagi pengguna dan relevan dengan fungsi inti aplikasi.

Aplikasi akan diizinkan untuk mengakses lokasi menggunakan izin layanan latar depan (ketika aplikasi hanya memiliki akses latar depan, misalnya "saat digunakan") jika penggunaan:

- telah dimulai sebagai kelanjutan dari tindakan yang dimulai pengguna dalam aplikasi, dan
- dihentikan langsung setelah kasus penggunaan yang dimaksud dari tindakan yang dimulai pengguna telah diselesaikan oleh aplikasi.

Aplikasi yang didesain khusus untuk anak-anak harus mematuhi kebijakan [Didesain untuk Keluarga](#).

## Izin Akses Semua File

File dan atribut direktori di perangkat pengguna dianggap sebagai data pengguna yang bersifat pribadi dan sensitif berdasarkan kebijakan [Informasi Pribadi dan Sensitif](#), serta persyaratan berikut:

- Aplikasi hanya boleh meminta akses ke penyimpanan perangkat yang benar-benar dibutuhkan agar aplikasi dapat berfungsi, dan tidak boleh meminta akses ke penyimpanan perangkat atas nama pihak ketiga mana pun untuk tujuan apa pun yang tidak terkait dengan fungsi aplikasi penting yang terlihat oleh pengguna.
- Perangkat Android yang menjalankan versi R (Android 11, API Level 30) atau yang lebih baru akan memerlukan izin [MANAGE\\_EXTERNAL\\_STORAGE](#) untuk mengelola akses di penyimpanan bersama. Semua aplikasi yang menargetkan versi R dan meminta akses secara luas ke penyimpanan bersama ("Akses semua file") harus berhasil melalui peninjauan akses yang sesuai sebelum dipublikasikan. Aplikasi yang diperbolehkan menggunakan izin ini harus secara jelas meminta pengguna mengaktifkan "Akses semua file" untuk aplikasi mereka dalam setelan "Akses aplikasi khusus". Untuk mengetahui informasi selengkapnya tentang persyaratan versi R, baca [artikel bantuan ini](#).

## Penyalahgunaan Perangkat dan Jaringan

Kami tidak mengizinkan aplikasi yang mengganggu, mengacaukan, merusak, atau mengakses dengan cara yang tidak sah perangkat pengguna, perangkat atau komputer lain, server, jaringan, application programming interface (API), atau layanan, termasuk tetapi tidak terbatas pada aplikasi lain pada perangkat, layanan Google apa pun, atau jaringan operator yang sah.

Aplikasi di Google Play harus mematuhi persyaratan pengoptimalan sistem Android default yang didokumentasikan dalam [Pedoman kualitas Aplikasi Inti untuk Google Play](#).

Aplikasi yang didistribusikan melalui Google Play tidak boleh memodifikasi, mengganti, atau mengupdate sendiri menggunakan metode apa pun selain mekanisme update Google Play. Selain itu, aplikasi tidak boleh mendownload kode yang dapat dieksekusi (misalnya file dex, JAR, .so) dari sumber lain selain Google Play. Pembatasan ini tidak berlaku untuk kode yang dijalankan di mesin virtual dan memiliki akses terbatas ke Android API (seperti JavaScript di webview atau browser).

Kami tidak mengizinkan kode yang menyebabkan atau mengeksploitasi kerentanan keamanan. Lihat [Program Peningkatan Keamanan Aplikasi](#) untuk mencari tahu masalah keamanan terbaru yang dilaporkan kepada developer.

Berikut beberapa contoh pelanggaran umum:

- Aplikasi yang menghalangi atau mengganggu aplikasi lain agar tidak bisa menampilkan iklan.
- Aplikasi untuk mencurangi game yang memengaruhi alur game aplikasi lain.
- Aplikasi yang memfasilitasi atau memberikan petunjuk peretasan layanan, software atau hardware, maupun mengakali perlindungan keamanan.
- Aplikasi yang mengakses atau menggunakan layanan maupun API dengan cara yang melanggar persyaratan layanannya.
- Aplikasi yang tidak [memenuhi syarat untuk diberi akses](#) dan mencoba mengabaikan [pengelolaan daya sistem](#).
- Aplikasi yang memfasilitasi layanan proxy kepada pihak ketiga hanya dapat melakukannya dalam aplikasi jika layanan tersebut merupakan tujuan utama aplikasi yang terlihat oleh pengguna.
- Aplikasi atau kode pihak ketiga (misalnya SDK) yang mendownload kode yang dapat dieksekusi, seperti file dex atau kode native, dari sumber selain Google Play.
- Aplikasi yang menginstal aplikasi lain pada perangkat tanpa izin pengguna.
- Aplikasi yang menautkan ke atau memfasilitasi distribusi atau penginstalan software berbahaya.

## Perilaku Menipu

Kami tidak mengizinkan aplikasi yang berupaya menipu pengguna atau memfasilitasi perilaku tidak jujur, termasuk tetapi tidak terbatas pada aplikasi yang dipastikan mustahil secara fungsional. Aplikasi harus memberikan pengungkapan, deskripsi, dan gambar/video yang akurat tentang fungsinya di semua bagian metadata. Aplikasi tidak boleh berupaya meniru fungsi atau peringatan dari sistem operasi atau aplikasi lain. Setiap perubahan pada setelan perangkat harus dilakukan dengan sepengetahuan dan seijin pengguna, serta dapat dikembalikan ke setelan semula oleh pengguna.

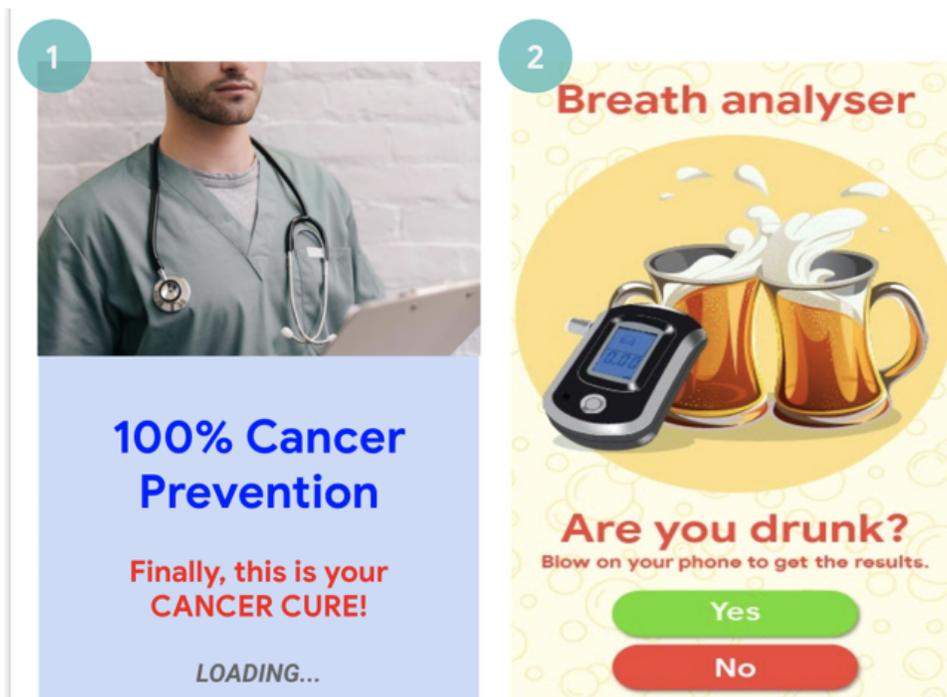
## Klaim Menyesatkan

Kami tidak mengizinkan aplikasi yang berisi informasi atau klaim yang menyesatkan atau palsu, termasuk dalam deskripsi, judul, ikon, dan screenshot.

Berikut beberapa contoh pelanggaran umum:

- Aplikasi yang memberikan pernyataan tidak benar tentang, atau tidak secara jelas dan akurat mendeskripsikan, fungsinya:

- Aplikasi yang mengklaim sebagai game balapan dalam deskripsi dan screenshot, tetapi sebenarnya adalah game blok puzzle yang menggunakan gambar mobil.
- Aplikasi yang mengklaim sebagai aplikasi antivirus, tetapi hanya berisi panduan teks yang menjelaskan cara menghapus virus.
- Nama aplikasi atau developer yang memberikan pernyataan tidak benar tentang status atau performa mereka saat ini di Play. (Mis. "Pilihan Editor," "Aplikasi Nomor 1," "Berbayar - Populer").
- Aplikasi yang memiliki konten atau fungsi terkait kesehatan atau medis yang menyesatkan atau berpotensi membahayakan.
- Aplikasi yang mengklaim fungsi yang tidak mungkin diimplementasikan (misalnya aplikasi pembasmi serangga), meskipun digambarkan sebagai trik tipuan, palsu, candaan, dll.
- Aplikasi yang dikategorikan dengan tidak benar, termasuk tetapi tidak terbatas pada rating aplikasi atau kategori aplikasi.
- Konten yang terbukti menipu dan dapat mengganggu proses pemungutan suara.
- Aplikasi yang memberikan klaim palsu terkait afiliasi dengan lembaga pemerintah atau menyediakan maupun memfasilitasi layanan pemerintah tanpa izin resmi.
- Aplikasi yang memberikan klaim palsu sebagai aplikasi resmi entitas ternama. Judul seperti "Justin Bieber Resmi" tidak diperbolehkan tanpa izin atau hak yang diperlukan.



- (1) Aplikasi ini menampilkan klaim terkait kesehatan atau medis (Menyembuhkan Kanker) yang menyesatkan  
 (2) Aplikasi ini mengklaim fungsi yang tidak mungkin diimplementasikan (menggunakan ponsel sebagai alat tes kadar alkohol melalui napas)

## Perubahan pada Setelan Perangkat yang Bersifat Menipu

Kami tidak mengizinkan aplikasi yang mengubah setelan atau fitur perangkat pengguna di luar aplikasi tanpa sepengetahuan dan persetujuan pengguna. Setelan dan fitur perangkat mencakup setelan browser dan sistem, bookmark, pintasan, ikon, widget, dan presentasi aplikasi di layar utama.

Selain itu, kami tidak mengizinkan:

- Aplikasi yang mengubah setelan atau fitur perangkat dengan persetujuan pengguna tetapi melakukannya dengan cara yang tidak mudah dikembalikan.
- Aplikasi atau iklan yang mengubah setelan atau fitur perangkat sebagai layanan kepada pihak ketiga atau untuk tujuan periklanan.
- Aplikasi yang menyesatkan pengguna untuk menghapus atau menonaktifkan aplikasi pihak ketiga atau mengubah setelan atau fitur perangkat.
- Aplikasi yang mendorong atau memberikan insentif kepada pengguna untuk menghapus atau menonaktifkan aplikasi pihak ketiga, atau mengubah setelan maupun fitur perangkat, kecuali merupakan bagian dari layanan keamanan yang dapat diverifikasi.

## Memfasilitasi Perilaku Tidak Jujur

Kami tidak mengizinkan aplikasi yang membantu pengguna untuk menyesatkan orang lain atau memiliki fungsi yang menipu dengan cara apa pun, termasuk tetapi tidak terbatas pada: aplikasi yang membuat atau memfasilitasi pembuatan kartu tanda pengenal, nomor jaminan sosial, paspor, ijazah, kartu kredit, dan SIM. Aplikasi harus memberikan pengungkapan, judul, deskripsi, dan gambar/video yang akurat terkait fungsi dan/atau kontennya, serta harus memiliki performa yang wajar dan akurat sesuai ekspektasi pengguna.

Resource aplikasi tambahan (misalnya, aset game) hanya boleh didownload jika diperlukan untuk penggunaan aplikasi oleh pengguna. Resource yang didownload harus mematuhi semua kebijakan Google Play, dan sebelum memulai proses download, aplikasi harus meminta persetujuan pengguna dan mengungkapkan ukuran download dengan jelas.

Klaim apa pun yang menyatakan bahwa aplikasi merupakan "trik tipuan", "untuk tujuan hiburan" (atau sinonim lainnya) tidak akan membebaskan aplikasi dari penerapan kebijakan kami.

Berikut beberapa contoh pelanggaran umum:

- Aplikasi yang meniru aplikasi atau situs lain untuk mengelabui pengguna agar mengungkapkan informasi pribadi atau autentikasi.
- Aplikasi yang menggambarkan atau menampilkan nomor telepon, kontak, alamat, atau informasi identitas pribadi aktual yang belum diverifikasi milik individu atau entitas yang tidak memberikan izin.
- Aplikasi dengan fungsi inti yang berbeda berdasarkan geografi pengguna, parameter perangkat, atau data lain yang bergantung pada pengguna, dan perbedaan tersebut tidak ditampilkan dengan jelas kepada pengguna di listingan Play Store.
- Aplikasi yang berubah secara signifikan dalam setiap versi tanpa memberi tahu pengguna (misalnya [bagian 'yang baru'](#)) dan yang mengupdate listingan Play Store.
- Aplikasi yang mencoba mengubah atau menyamarkan perilaku selama peninjauan.
- Aplikasi dengan hasil download yang difasilitasi oleh jaringan penayangan konten (CDN) yang gagal meminta izin pengguna dan mengungkapkan ukuran download sebelum download dilakukan.

## Media yang Dimanipulasi

Kami tidak mengizinkan aplikasi yang memberikan atau membantu membuat informasi maupun klaim yang menyesatkan atau palsu yang disampaikan melalui gambar, video, dan/atau teks. Kami tidak mengizinkan aplikasi yang dimaksudkan untuk memberikan atau menyebarkan citra, video, dan/atau teks yang terbukti menyesatkan atau menipu, yang dapat menimbulkan bahaya terkait peristiwa sensitif, politik, masalah sosial, atau masalah lain yang menjadi perhatian publik.

Aplikasi yang memanipulasi atau mengubah media, di luar penyesuaian yang dapat diterima secara editorial dan konvensional terkait kejelasan dan kualitas, harus mengungkapkan dengan jelas atau memberikan watermark pada media yang diubah jika aplikasi dirasa dapat membingungkan orang-orang bahwa media telah diubah. Pengecualian mungkin diberikan untuk minat publik atau satire yang jelas atau parodi.

Berikut beberapa contoh pelanggaran umum:

- Aplikasi yang menambahkan tokoh masyarakat pada demonstrasi selama peristiwa yang bersifat sensitif secara politik.
- Aplikasi yang menggunakan tokoh masyarakat atau media dari suatu peristiwa sensitif untuk mengiklankan media yang mengubah kemampuan dalam listingan Play Store aplikasi.
- Aplikasi yang mengubah klip media untuk meniru siaran berita.



(1) Aplikasi ini menyediakan fungsi yang dapat mengubah klip media untuk meniru siaran berita, dan menambahkan tokoh terkenal atau tokoh masyarakat pada klip tanpa memberikan watermark.

## Pernyataan Tidak Benar

Kami tidak mengizinkan aplikasi atau akun developer yang:

- meniru identitas orang atau organisasi apa pun, atau memberikan pernyataan tidak benar atau menyembunyikan kepemilikan atau tujuan utamanya.
- terlibat dalam aktivitas terkoordinasi untuk menyesatkan pengguna. Hal ini termasuk, tetapi tidak terbatas pada, aplikasi atau akun developer yang memberikan pernyataan tidak benar atau menyembunyikan negara asalnya, atau yang menargetkan konten kepada pengguna di negara lain.
- berkoordinasi dengan aplikasi, situs, developer, atau akun lain untuk menyembunyikan atau memberikan pernyataan tidak benar terkait identitas developer atau aplikasi atau detail materi lainnya, yang mana konten aplikasi berkaitan dengan politik, masalah sosial, atau masalah yang menjadi perhatian publik.

## Malware

Malware adalah semua kode yang dapat membahayakan pengguna, data pengguna, atau perangkat. Malware meliputi, tetapi tidak terbatas pada, Aplikasi yang Berpotensi Membahayakan (PHA), biner, atau modifikasi framework, yang terdiri dari kategori seperti trojan, phishing, serta aplikasi spyware, dan kami akan terus memperbarui dan menambahkan kategori baru.

## Malware

Kebijakan Malware kami cukup sederhana; ekosistem Android, termasuk Google Play Store dan perangkat pengguna, harus bebas dari perilaku berbahaya (yaitu malware). Dengan prinsip dasar ini, kami berusaha untuk menyediakan ekosistem Android yang aman bagi pengguna dan perangkat Android mereka.

Meskipun jenis dan kemampuannya bervariasi, malware biasanya memiliki salah satu tujuan berikut:

- Mengganggu integritas perangkat pengguna.
- Mendapatkan kontrol atas perangkat pengguna.
- Mengaktifkan operasi yang dapat dikontrol jarak jauh agar penyerang dapat mengakses, menggunakan, atau memanfaatkan perangkat yang terinfeksi.
- Mengirim data pribadi atau kredensial dari perangkat tanpa pengungkapan dan persetujuan yang memadai.
- Menyebarkan spam atau perintah dari perangkat terinfeksi untuk memengaruhi jaringan atau perangkat lain.

- Menipu pengguna.

Aplikasi, biner, atau modifikasi framework dapat Berpotensi Membahayakan, dan karena itu dapat menghasilkan perilaku berbahaya, meskipun tidak dimaksudkan untuk membahayakan. Ini karena aplikasi, biner, atau modifikasi framework dapat berfungsi secara berbeda tergantung berbagai variabel. Oleh karena itu, yang membahayakan bagi suatu perangkat Android belum tentu membahayakan bagi perangkat Android lain. Misalnya, suatu perangkat yang menjalankan versi Android terbaru tidak akan terpengaruh oleh aplikasi berbahaya yang menggunakan API usang untuk menjalankan perilaku berbahaya. Namun, perangkat yang masih menjalankan versi Android paling lama mungkin berisiko. Aplikasi, biner, atau modifikasi framework ditandai sebagai malware atau PHA jika kesemuanya jelas membahayakan beberapa atau semua pengguna dan perangkat Android.

Kategori malware, di bawah ini, merefleksikan keyakinan dasar kami bahwa pengguna harus memahami cara perangkat mereka dimanfaatkan dan mendorong ekosistem aman yang memungkinkan inovasi tangguh serta pengalaman pengguna yang tepercaya.

Buka [Google Play Protect](#) untuk mengetahui informasi selengkapnya.

## Backdoor (Pintu belakang)

Kode yang mengizinkan dieksekusinya operasi jarak jauh yang tidak diinginkan dan berpotensi membahayakan perangkat.

Operasi ini mungkin menyertakan perilaku yang akan menempatkan aplikasi, biner, atau modifikasi framework masuk ke dalam salah satu kategori malware lainnya jika otomatis dijalankan. Secara umum, backdoor (pintu belakang) dapat dideskripsikan sebagai operasi yang berpotensi membahayakan yang dapat terjadi pada suatu perangkat. Oleh karena itu, operasi tersebut tidak benar-benar sesuai dengan kategori seperti penipuan tagihan atau spyware komersial. Akibatnya, sebagian backdoor (pintu belakang), dalam situasi tertentu, dianggap sebagai kerentanan oleh Google Play Protect.

## Penipuan Tagihan

Kode yang otomatis membebankan biaya kepada pengguna dengan cara yang sengaja menipu.

Penipuan tagihan seluler terbagi menjadi penipuan SMS, penipuan Telepon, dan penipuan Pulsa.

### *Penipuan SMS*

Kode yang membebankan biaya kepada pengguna untuk mengirim SMS premium tanpa izin, atau mencoba untuk menyamarkan aktivitas SMS-nya dengan menyembunyikan perjanjian pengungkapan atau pesan SMS dari operator seluler yang memberi tahu pengguna tentang tagihan atau konfirmasi langganan.

Beberapa kode, meskipun secara teknis mengungkapkan perilaku pengiriman SMS, menunjukkan perilaku tambahan yang mengakomodasi penipuan SMS. Contohnya termasuk menyembunyikan bagian perjanjian pengungkapan dari pengguna sehingga tidak dapat dibaca, dan terkadang menyembunyikan pesan SMS dari operator seluler yang memberi tahu pengguna tentang tagihan atau konfirmasi langganan.

### *Penipuan Telepon*

Kode yang membebankan biaya kepada pengguna dengan melakukan panggilan ke nomor premium tanpa izin pengguna.

### *Penipuan Pulsa*

Kode yang mengelabui pengguna agar berlangganan atau membeli konten melalui tagihan ponsel.

Penipuan Pulsa meliputi semua jenis penagihan kecuali SMS premium dan panggilan premium. Contohnya termasuk tagihan operator langsung, titik akses nirkabel (WAP), dan transfer pulsa seluler. Penipuan WAP adalah salah satu jenis penipuan Pulsa paling umum. Penipuan WAP dapat termasuk mengelabui pengguna agar mengklik tombol pada WebView transparan yang diam-diam dimuat. Setelah melakukan tindakan ini, langganan berulang akan dimulai, dan SMS atau email konfirmasi sering kali dibajak agar pengguna tidak menyadari transaksi keuangan yang terjadi.

## Stalkerware

Kode yang mentransmisikan informasi pribadi dari perangkat tanpa pemberitahuan atau persetujuan yang memadai dan tidak menampilkan notifikasi persisten yang menjelaskan bahwa hal tersebut terjadi.

Aplikasi stalkerware biasanya mentransmisikan data kepada pihak selain penyedia aplikasi yang berpotensi membahayakan (PHA).

Bentuk yang dapat diterima dari aplikasi ini dapat digunakan orang tua untuk melacak anak-anaknya. Namun, aplikasi ini tidak dapat digunakan untuk melacak seseorang (misalnya pasangan) tanpa sepengetahuan atau seizin mereka, kecuali

ada notifikasi persisten yang ditampilkan saat data sedang ditransmisikan.

Aplikasi yang boleh didistribusikan di Play Store dengan fitur pelacakan dan pelaporan hanyalah aplikasi yang mematuhi kebijakan, yang didesain dan dipasarkan secara khusus untuk pemantauan oleh orang tua (termasuk keluarga) atau pengelolaan perusahaan, asalkan aplikasi tersebut sepenuhnya mematuhi persyaratan yang dijelaskan di bawah.

Aplikasi non-stalkerware yang didistribusikan di Play Store dan memiliki fitur untuk memantau atau melacak perilaku pengguna pada perangkat minimal harus memenuhi persyaratan berikut:

- Aplikasi tidak boleh berfungsi sebagai alat untuk memata-matai atau melakukan pengintaian rahasia.
- Aplikasi tidak boleh menyembunyikan perilaku pelacakan terselubung atau berupaya untuk menyesatkan pengguna tentang fungsi tersebut.
- Aplikasi harus menunjukkan ikon unik dan notifikasi persisten yang jelas mengidentifikasi aplikasi kepada pengguna.
- Aplikasi dan listing aplikasi di Google Play tidak boleh memberikan cara apa pun untuk mengaktifkan atau mengakses fungsi yang melanggar persyaratan ini, seperti menautkan ke APK yang melanggar dan dihosting di luar Google Play.
- Anda sepenuhnya bertanggung jawab untuk menetapkan keabsahan aplikasi dalam lokal targetnya. Aplikasi yang ditetapkan melanggar hukum di lokasi tempat publikasinya akan dihapus.

## Denial of Service (DoS)

Kode yang tanpa sepengetahuan pengguna mengeksekusi serangan denial-of-service (DoS) atau merupakan bagian dari serangan DoS yang didistribusikan pada sistem dan resource lainnya.

Misalnya, serangan ini dapat terjadi melalui pengiriman permintaan HTTP bervolume tinggi untuk menghasilkan muatan berlebih pada server jarak jauh.

## Downloader Berbahaya

Kode yang sebenarnya tidak berpotensi membahayakan, tetapi mendownload aplikasi yang berpotensi membahayakan (PHA) lainnya.

Kode bisa berupa downloader berbahaya jika:

- Ada alasan untuk meyakini bahwa kode dibuat untuk menyebarkan PHA dan kode telah mendownload PHA atau berisi kode yang dapat mendownload atau menginstal aplikasi; atau
- Setidaknya 5% aplikasi yang didownload oleh kode merupakan PHA dengan batas minimum 500 download aplikasi yang diamati (25 hasil download PHA yang diamati).

Browser utama dan aplikasi berbagi file tidak dianggap sebagai downloader berbahaya selama:

- Browser dan aplikasi tidak mendorong download tanpa interaksi pengguna; dan
- Semua download PHA dimulai dengan izin pengguna.

## Ancaman Non-Android

Kode yang berisi ancaman non-Android.

Aplikasi ini tidak membahayakan pengguna atau perangkat Android, tetapi berisi komponen yang berpotensi membahayakan platform lainnya.

## Phishing

Kode yang seolah-olah berasal dari sumber tepercaya, meminta kredensial autentikasi atau informasi penagihan pengguna, dan mengirimkan data tersebut kepada pihak ketiga. Kategori ini juga berlaku pada kode yang mengintersep transmisi kredensial pengguna saat dalam pengiriman.

Target umum phishing meliputi kredensial perbankan, nomor kartu kredit, dan kredensial akun online untuk jaringan sosial dan game.

## Penyalahgunaan Hak Istimewa yang Ditingkatkan

Kode yang mengganggu integritas sistem dengan merusak sandbox aplikasi, mendapatkan hak istimewa yang ditingkatkan, atau mengubah maupun menonaktifkan akses ke fungsi terkait keamanan inti.

Contohnya mencakup:

- Aplikasi yang melanggar model izin Android, atau mencuri kredensial (seperti token OAuth) dari aplikasi lain.
- Aplikasi yang menyalahgunakan fitur agar aplikasi tidak dapat di-uninstal atau dihentikan.
- Aplikasi yang menonaktifkan SELinux.

Aplikasi eskalasi akses yang melakukan root pada perangkat tanpa izin pengguna diklasifikasikan sebagai aplikasi rooting.

## Ransomware

Kode yang mengambil sebagian atau seluruh kontrol perangkat atau data pada perangkat dan meminta pengguna membayar atau melakukan tindakan untuk mengambil kembali kontrol tersebut.

Beberapa ransomware mengenkripsi data pada perangkat dan meminta pembayaran untuk mendekripsi data dan/atau memanfaatkan fitur admin perangkat sehingga data tidak dapat dihapus oleh pengguna biasa. Contohnya mencakup:

- Membuat pengguna tidak dapat login ke perangkatnya dan meminta uang untuk memulihkan kontrol pengguna.
- Mengenkripsi data pada perangkat dan meminta pembayaran, seolah-olah untuk mendekripsi data.
- Memanfaatkan fitur pengelola kebijakan perangkat dan memblokir penghapusan oleh pengguna.

Kode yang didistribusikan dengan perangkat, yang tujuan utamanya adalah menggantikan pengelolaan perangkat, dapat dikecualikan dari kategori ransomware jika berhasil memenuhi persyaratan untuk pengelolaan dan penguncian yang aman, serta persyaratan izin dan pengungkapan pengguna yang memadai.

## Rooting

Kode yang melakukan root pada perangkat.

Ada perbedaan antara kode rooting tidak berbahaya dan berbahaya. Misalnya, aplikasi rooting tidak berbahaya akan memberi tahu pengguna sebelum melakukan root pada perangkat dan tidak akan menjalankan tindakan berpotensi membahayakan lainnya yang berlaku pada kategori aplikasi yang berpotensi membahayakan (PHA) lainnya.

Aplikasi rooting yang berbahaya bukan hanya tidak memberi tahu pengguna sebelum melakukan root pada perangkat, ataupun memberi tahu di awal terkait proses root ini, tetapi juga mengeksekusi tindakan lain yang termasuk dalam kategori aplikasi yang berpotensi membahayakan (PHA) lainnya.

## Spam

Kode yang mengirimkan pesan tidak diminta ke kontak pengguna atau menggunakan perangkat sebagai sarana untuk meneruskan penyebaran spam email.

## Spyware

Kode yang mentransmisikan data pribadi dari perangkat tanpa izin atau pemberitahuan yang memadai.

Misalnya, mentransmisikan informasi berikut tanpa pengungkapan atau dengan cara yang tidak diketahui pengguna dapat dianggap sebagai spyware:

- Daftar kontak
- Foto atau file lainnya dari kartu SD atau yang tidak dimiliki oleh aplikasi
- Konten dari email pengguna
- Log panggilan
- Log SMS
- Histori web atau bookmark browser dari browser default
- Informasi dari direktori /data/ aplikasi lain.

Perilaku yang dapat dianggap sebagai memata-matai pengguna juga dapat ditandai sebagai spyware. Misalnya, merekam audio atau merekam panggilan yang masuk ke ponsel, atau mencuri data aplikasi.

## Trojan

Kode yang tampak tidak berbahaya, seperti game yang mengklaim tidak memiliki fungsi selain sebagai game, tetapi melakukan tindakan yang tidak diinginkan terhadap pengguna.

Klasifikasi ini biasanya digunakan bersamaan dengan kategori Aplikasi yang Berpotensi Membahayakan (PHA) lainnya. Trojan memiliki komponen tidak berbahaya dan komponen membahayakan yang tersembunyi. Misalnya, game yang mengirimkan pesan SMS premium dari perangkat pengguna di latar belakang tanpa sepengetahuan pengguna.

## Catatan Terkait Aplikasi Tidak Umum

Aplikasi baru dan jarang dapat diklasifikasikan sebagai tidak umum jika Google Play Protect tidak memiliki cukup informasi untuk mengategorikannya sebagai aman. Hal ini tidak berarti bahwa aplikasi tersebut berbahaya, tetapi tanpa peninjauan lebih lanjut, aplikasi tersebut tidak dapat dikategorikan sebagai aman.

## Catatan terkait Kategori Backdoor (Pintu Belakang)

Klasifikasi kategori malware backdoor (pintu belakang) didasarkan pada cara kode berperilaku. Kode dapat diklasifikasikan sebagai backdoor (pintu belakang) bila memiliki perilaku yang membuatnya termasuk salah satu kategori malware lainnya jika otomatis dijalankan. Misalnya, jika suatu aplikasi memungkinkan pemuatan kode dinamis dan kode tersebut mengekstrak pesan teks, maka kode akan diklasifikasikan sebagai malware backdoor (pintu belakang).

Namun, jika suatu aplikasi memungkinkan eksekusi kode arbitrer dan kami tidak memiliki alasan untuk meyakini bahwa eksekusi kode ini ditambahkan untuk menjalankan perilaku membahayakan, aplikasi akan dianggap memiliki kerentanan, bukan malware backdoor (pintu belakang), dan developer akan diminta untuk menambahkan patch pada aplikasi.

## Software Seluler yang Tidak Diinginkan

Kebijakan ini dikembangkan dari Kebijakan Software yang Tidak Diinginkan Google dengan menguraikan prinsip-prinsip ekosistem Android dan Google Play Store. Software yang melanggar prinsip ini berpotensi membahayakan pengalaman pengguna, dan kami akan mengambil langkah-langkah untuk melindungi pengguna darinya.

### Software Seluler yang Tidak Diinginkan

Di Google, kami percaya jika fokus pada pengguna, semua hal lain akan mengikuti. Dalam [Prinsip-Prinsip Software](#) dan [Kebijakan Software yang Tidak Diinginkan](#), kami memberikan rekomendasi umum terkait software yang menyajikan pengalaman pengguna yang optimal. Kebijakan ini dikembangkan dari Kebijakan Software yang Tidak Diinginkan Google dengan menguraikan prinsip-prinsip ekosistem Android dan Google Play Store. Software yang melanggar prinsip ini berpotensi membahayakan pengalaman pengguna, dan kami akan mengambil langkah-langkah untuk melindungi pengguna darinya.

Seperti disebutkan dalam [Kebijakan Software yang Tidak Diinginkan](#), kami menemukan bahwa sebagian besar software yang tidak diinginkan menunjukkan satu atau beberapa karakteristik dasar yang sama:

- Bersifat menipu, menjanjikan proposisi nilai yang tidak dapat dipenuhi.
- Mencoba mengelabui pengguna agar menginstalnya, atau menumpang pada penginstalan software lain.
- Tidak memberi tahu pengguna tentang semua prinsip dan fungsi pentingnya.
- Memengaruhi sistem pengguna dengan cara yang tidak diketahui.
- Mengumpulkan atau mentransmisikan informasi pribadi tanpa sepengetahuan pengguna.
- Mengumpulkan atau mentransmisikan informasi pribadi tanpa penanganan yang aman (misalnya transmisi melalui HTTPS)
- Disertakan dalam software lain dan keberadaannya tidak diungkapkan.

Pada perangkat seluler, software merupakan kode yang berbentuk aplikasi, biner, modifikasi framework, dll. Untuk mencegah software yang membahayakan ekosistem software atau mengganggu pengalaman pengguna, kami akan mengambil tindakan terhadap kode yang melanggar prinsip-prinsip ini.

Di bawah ini, kami mengembangkan Kebijakan Software yang Tidak Diinginkan untuk memperluas penerapannya pada software seluler. Sehubungan dengan kebijakan tersebut, kami akan terus menyempurnakan kebijakan Software Seluler yang Tidak Diinginkan ini untuk menangani jenis penyalahgunaan baru.

### Perilaku yang transparan dan pengungkapan yang jelas

*Semua kode harus memenuhi komitmen yang dibuat kepada pengguna. Aplikasi harus menyediakan semua fungsi yang disampaikan. Aplikasi tidak boleh membingungkan pengguna.*

- Aplikasi harus menyatakan fungsi dan tujuannya dengan jelas.
- Sampaikan secara jelas dan eksplisit kepada pengguna tentang perubahan sistem yang akan dilakukan oleh aplikasi. Izinkan pengguna untuk meninjau dan menyetujui semua opsi penginstalan dan perubahan yang signifikan.
- Software tidak boleh memberikan pernyataan tidak benar tentang status perangkat kepada pengguna, misalnya dengan mengatakan bahwa sistem berada dalam kondisi keamanan kritis atau terinfeksi virus.
- Jangan gunakan aktivitas tidak valid yang didesain untuk meningkatkan traffic iklan dan/atau konversi.
- Kami tidak mengizinkan aplikasi yang menyesatkan pengguna dengan meniru identitas orang lain (misalnya developer, perusahaan, entitas lain) atau aplikasi lain. Jangan menyiratkan bahwa aplikasi Anda terkait dengan atau diberi izin oleh seseorang yang sebenarnya tidak terlibat.

Contoh pelanggaran:

- Penipuan iklan
- Peniruan identitas

### Lindungi data pengguna

*Sampaikan secara jelas dan transparan tentang akses, penggunaan, pengumpulan, serta aktivitas berbagi data pengguna yang bersifat pribadi dan sensitif. Penggunaan data pengguna harus mematuhi semua Kebijakan Data Pengguna yang relevan, jika berlaku, dan mengambil semua tindakan pencegahan untuk melindungi data.*

- Berikan kesempatan kepada pengguna untuk menyetujui pengumpulan data sebelum Anda mulai mengumpulkan dan mengirimkannya dari perangkat mereka, termasuk data tentang akun pihak ketiga, email, nomor telepon, aplikasi terinstal, file, lokasi, serta data pribadi dan sensitif lainnya yang pengumpulannya tidak diketahui oleh pengguna.
- Pengumpulan data pengguna yang bersifat pribadi dan sensitif harus ditangani dengan aman, termasuk ditransmisikan menggunakan kriptografi modern (misalnya, melalui HTTPS).
- Software, termasuk aplikasi seluler, hanya boleh mentransmisikan data pengguna yang bersifat pribadi dan sensitif ke server sebagaimana terkait dengan fungsi aplikasi.

Contoh pelanggaran:

- Pengumpulan Data (cf [Spyware](#))
- Penyalahgunaan Izin Terbatas

Contoh Kebijakan Data Pengguna:

- [Kebijakan Data Pengguna Google Play](#)
- [Kebijakan Data Pengguna Persyaratan GMS](#)
- [Kebijakan Data Pengguna Layanan Google API](#)

### Jangan merusak pengalaman aplikasi seluler

*Pengalaman pengguna harus jelas, mudah dipahami, dan didasarkan pada pilihan jelas yang dibuat oleh pengguna. Pengalaman harus menghadirkan proposisi nilai yang jelas untuk pengguna, dan tidak menyimpang dari pengalaman pengguna yang diiklankan atau diinginkan.*

- Jangan tampilkan iklan dengan cara yang tidak diharapkan oleh pengguna, termasuk menghalangi atau mengganggu kegunaan fungsi perangkat, atau menampilkannya di luar lingkungan aplikasi yang memicunya tanpa cara yang jelas untuk menutupnya serta izin dan atribusi yang memadai.
- Aplikasi tidak boleh mengganggu aplikasi lain atau kegunaan perangkat
- Jika berlaku, proses uninstal harus jelas.
- Software seluler tidak boleh meniru perintah dari OS perangkat atau aplikasi lain. Jangan menyembunyikan peringatan yang ditujukan kepada pengguna dari aplikasi lain atau sistem operasi, terutama yang memberi tahu pengguna tentang perubahan pada OS.

Contoh pelanggaran:

- Iklan yang mengganggu
- Penggunaan yang Tidak Sah atau Imitasi Fungsi Sistem

## Penipuan Iklan

Penipuan iklan dilarang tanpa pengecualian. Interaksi iklan yang dibuat untuk mengelabui jaringan iklan agar percaya bahwa traffic berasal dari minat pengguna asli adalah penipuan iklan, yang merupakan bentuk [traffic tidak valid](#). Penipuan iklan dapat disebabkan oleh developer yang mengimplementasikan iklan dengan cara yang dilarang, seperti menampilkan iklan tersembunyi, mengklik iklan secara otomatis, mengubah atau memodifikasi informasi, atau memanfaatkan tindakan yang tidak dilakukan manusia (spider, bot, dsb.), atau aktivitas manusia yang didesain untuk menghasilkan traffic iklan tidak valid. Traffic tidak valid dan penipuan iklan dapat membahayakan pengiklan, developer, dan pengguna, serta menyebabkan hilangnya kepercayaan jangka panjang pada ekosistem Iklan seluler.

Berikut beberapa contoh pelanggaran umum:

- Aplikasi yang merender iklan yang tidak terlihat oleh pengguna.
- Aplikasi yang secara otomatis menghasilkan klik pada iklan tanpa niat dari pengguna, atau yang menghasilkan traffic jaringan yang setara untuk memberikan kredit klik dengan cara yang menipu.
- Aplikasi yang mengirimkan klik atribusi penginstalan palsu untuk mendapatkan bayaran atas penginstalan yang tidak berasal dari jaringan pengirim.
- Aplikasi yang menampilkan iklan pop-up saat pengguna sedang tidak berada dalam antarmuka aplikasi.

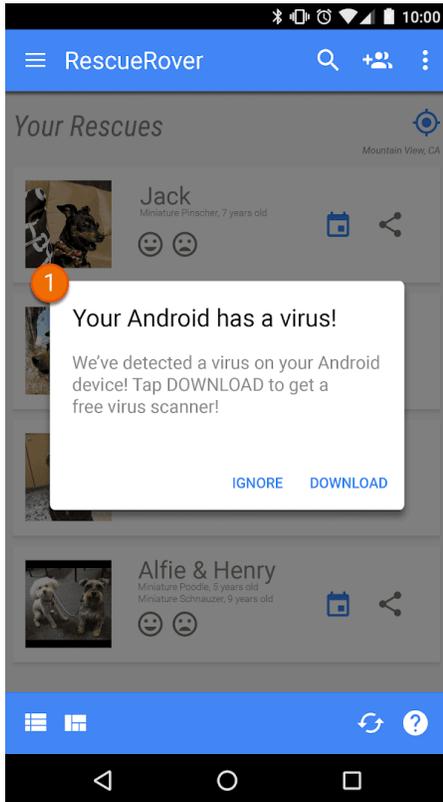
- Pernyataan palsu tentang inventaris iklan oleh aplikasi, misalnya aplikasi yang menginformasikan pada jaringan iklan bahwa aplikasi tersebut berjalan di perangkat iOS padahal sebenarnya berjalan di perangkat Android; aplikasi yang memberikan pernyataan tidak benar tentang nama paket yang dimonetisasi.

## Penggunaan yang Tidak Sah atau Imitasi Fungsi Sistem

Kami tidak mengizinkan aplikasi atau iklan yang meniru atau mengganggu fungsi sistem, seperti notifikasi atau peringatan. Notifikasi level sistem hanya dapat digunakan untuk fitur yang tidak terpisahkan dari sebuah aplikasi, seperti aplikasi maskapai penerbangan yang menginformasikan penawaran khusus kepada pengguna, atau game yang menginformasikan promosi dalam game kepada pengguna.

Berikut beberapa contoh pelanggaran umum:

- Aplikasi atau iklan yang ditayangkan melalui notifikasi atau peringatan sistem:



① Notifikasi sistem yang ditampilkan dalam aplikasi ini digunakan untuk menayangkan iklan.

Untuk melihat contoh tambahan terkait iklan, baca [Kebijakan iklan](#).

## Peniruan identitas

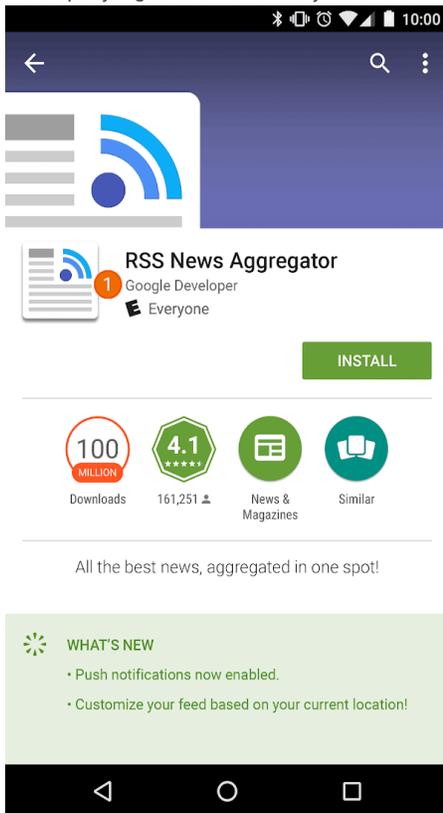
Developer yang meniru identitas atau aplikasi orang lain akan menyesatkan pengguna dan memberikan dampak negatif pada komunitas developer. Kami melarang aplikasi yang menyesatkan pengguna dengan cara meniru identitas orang lain.

### Peniruan identitas

Kami tidak mengizinkan aplikasi yang menyesatkan pengguna dengan meniru identitas orang lain (misalnya developer, perusahaan, entitas lain) atau aplikasi lain. Jangan menyiratkan bahwa aplikasi Anda terkait dengan atau diberi izin oleh seseorang yang sebenarnya tidak terlibat. Berhati-hatilah untuk tidak menggunakan ikon, deskripsi, judul, atau elemen dalam aplikasi yang dapat menyesatkan pengguna mengenai hubungan aplikasi Anda dengan orang atau aplikasi lain.

Berikut beberapa contoh pelanggaran umum:

- Developer yang secara keliru menyiratkan hubungan dengan perusahaan/developer lain:



① Nama developer yang tercantum untuk aplikasi ini menunjukkan hubungan resmi dengan Google, padahal sebenarnya tidak demikian.

- Judul dan ikon aplikasi yang sangat mirip dengan produk atau layanan yang sudah ada, sehingga dapat menyesatkan

✓	 Google Maps	 Google+	 YouTube	 Twitter
✗	 Google Maps Navigator	 Google+ Sharify	 YouTube Aggregator	 TwitterPro

## Monetisasi dan Iklan

Google Play mendukung berbagai strategi monetisasi untuk memberikan keuntungan bagi developer dan pengguna, termasuk distribusi berbayar, produk dalam aplikasi, langganan, dan model berbasis iklan. Untuk memastikan pengalaman pengguna yang terbaik, Anda wajib mematuhi kebijakan berikut.

## Pembayaran

Aplikasi yang menggunakan mekanisme pembelian di toko maupun di dalam aplikasi harus mematuhi pedoman berikut:

**Pembelian di toko:** Developer yang mengenakan biaya untuk aplikasi dan download dari Google Play harus menggunakan sistem pembayaran milik Google Play.

**Pembelian di dalam aplikasi:**

- Developer yang menawarkan produk dalam game yang didownload di Google Play, atau memberikan akses ke konten game, harus menggunakan [Penagihan via Google Play](#) sebagai metode pembayaran.
- Developer yang menawarkan produk dalam kategori lain dari aplikasi yang didownload di Google Play harus menggunakan [Penagihan via Google Play](#) sebagai metode pembayaran, kecuali untuk beberapa hal berikut:
  - Pembayaran hanya untuk produk fisik

- Pembayaran dilakukan untuk konten digital yang dapat digunakan di luar aplikasi tersebut (misalnya, lagu yang dapat diputar di pemutar musik lainnya).
- Mata uang virtual hanya boleh digunakan di dalam aplikasi atau untuk game yang dibeli.
- Developer tidak boleh memberikan informasi yang menyesatkan pengguna mengenai aplikasi yang mereka jual, ataupun tentang layanan dalam aplikasi, barang, konten, atau fungsi apa pun yang ditawarkan untuk dibeli. Jika deskripsi produk Anda di Google Play merujuk pada fitur dalam aplikasi yang mungkin membutuhkan biaya tertentu atau biaya tambahan, deskripsi harus jelas memberi tahu pengguna bahwa mereka perlu membayar untuk mengakses fitur tersebut.
- Aplikasi yang menawarkan mekanisme untuk menerima item virtual acak dari suatu pembelian (misalnya 'loot box') harus jelas mengungkapkan peluang pengguna untuk menerima item tersebut sebelum membelinya.

#### **Berikut beberapa contoh produk yang didukung oleh Penagihan via Google Play:**

- **Produk game virtual**, termasuk koin, permata, tambahan nyawa atau giliran, item atau peralatan khusus, karakter atau avatar, level atau waktu bermain tambahan.
- **Fungsi atau konten aplikasi**, misalnya aplikasi versi bebas iklan atau fitur baru yang tidak tersedia dalam versi gratis.
- **Layanan berlangganan**, misalnya streaming musik, video, buku, atau layanan media lainnya; publikasi digital, termasuk jika dipaketkan dengan edisi fisik; serta layanan jaringan sosial.
- **Produk software cloud**, meliputi layanan penyimpanan data, software produktivitas bisnis, dan software pengelolaan keuangan.

#### **Berikut beberapa contoh produk yang saat ini tidak didukung oleh Penagihan via Google Play:**

- **Merchandise retail**, misalnya bahan makanan, pakaian, peralatan rumah tangga, dan perangkat elektronik.
- **Tarif layanan**, meliputi layanan taksi dan transportasi, jasa kebersihan, layanan antar makanan, tiket pesawat, dan tiket acara.
- **Biaya keanggotaan sekali bayar atau iuran berulang**, meliputi keanggotaan gym, program loyalitas, atau klub yang menawarkan aksesoris, pakaian, atau produk fisik lainnya.
- **Pembayaran hanya sekali**, meliputi pembayaran peer-to-peer, lelang online, dan donasi.
- **Pembayaran tagihan elektronik**, meliputi tagihan kartu kredit, utilitas, dan layanan TV kabel atau telekomunikasi.

Perlu diperhatikan bahwa kami menawarkan Google Play API untuk aplikasi yang menjual layanan dan produk fisik. Untuk informasi selengkapnya, buka [halaman developer Google Play](#).

## Langganan

Sebagai developer, Anda dilarang menyesatkan pengguna tentang konten atau layanan langganan apa pun yang ditawarkan dalam aplikasi Anda. Pastikan semuanya disampaikan dengan jelas dalam setiap promosi dalam aplikasi atau layar pembuka.

**Di aplikasi Anda:** Anda harus bersikap transparan tentang penawaran Anda. Hal ini mencakup pernyataan yang eksplisit tentang persyaratan penawaran Anda, biaya langganan, frekuensi siklus penagihan, dan apakah langganan diwajibkan untuk menggunakan aplikasi. Pengguna tidak perlu melakukan tindakan apa pun untuk meninjau informasi tersebut.

**Berikut beberapa contoh pelanggaran umum:**

- Langganan bulanan yang tidak memberi tahu pengguna bahwa perpanjangan dan pembayaran langganan akan dilakukan secara otomatis setiap bulan.
- Langganan tahunan yang dengan jelas hanya menampilkan harga yang berkaitan dengan biaya bulanan.
- Persyaratan dan harga langganan yang tidak sepenuhnya dilokalkan.
- Promosi dalam aplikasi yang tidak menunjukkan dengan jelas bahwa pengguna dapat mengakses konten tanpa langganan (jika tersedia).
- Nama SKU yang tidak menyampaikan sifat langganan secara akurat, seperti "Uji Coba Gratis" untuk langganan dengan biaya berulang otomatis.

**1** Get AnalyzeAPP Premium

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

2	12 months	6 months	1 month
	\$9.16/mo Save 35%!	\$12.50/mo Save 11%! MOST POPULAR PLAN	\$14.00/mo

**3** Try for \$12.50!

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

- ① Tombol tolak tidak terlihat jelas dan pengguna mungkin tidak memahami bahwa fungsi aplikasi dapat diakses tanpa perlu menerima penawaran langganan.
- ② Penawaran hanya menampilkan harga yang berkaitan dengan biaya bulanan, dan pengguna mungkin tidak mengetahui jika akan dikenai biaya setara dengan enam bulan langganan ketika berlangganan.
- ③ Penawaran hanya menampilkan harga pengenalan, dan pengguna mungkin tidak mengetahui bahwa mereka akan otomatis dikenai biaya pada akhir periode pengenalan.
- ④ Penawaran seharusnya dilokalkan dalam bahasa yang sama dengan yang digunakan pada persyaratan dan ketentuan sehingga pengguna dapat memahami keseluruhan penawaran.

## Uji Coba Gratis & Penawaran Harga Perkenalan

Sebelum pengguna terdaftar dalam langganan Anda: Anda harus memberitahukan persyaratan penawaran dengan jelas dan akurat, termasuk durasi, harga, dan deskripsi konten atau layanan yang dapat diakses. Pastikan Anda memberi tahu pengguna bagaimana dan kapan uji coba gratis akan dikonversi menjadi langganan berbayar, berapa biaya langganan berbayar, dan bahwa pengguna dapat membatalkan langganan tersebut jika tidak ingin mengonversinya menjadi langganan berbayar.

Berikut beberapa contoh pelanggaran umum:

- Penawaran yang tidak memberi tahu dengan jelas tentang durasi uji coba gratis atau harga pengenalan.
- Penawaran yang tidak memberi tahu dengan jelas bahwa pengguna akan otomatis terdaftar dalam langganan berbayar pada akhir periode penawaran.
- Penawaran yang tidak memberi tahu dengan jelas bahwa pengguna dapat mengakses konten tanpa uji coba (jika tersedia).
- Harga dan persyaratan penawaran yang tidak sepenuhnya dilokalkan.

**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 Tombol tolak tidak terlihat jelas dan pengguna mungkin tidak memahami bahwa fungsi aplikasi dapat diakses tanpa perlu mendaftar untuk uji coba gratis.
- ② Penawaran menekankan pada uji coba gratis dan pengguna mungkin tidak mengetahui bahwa mereka akan otomatis dikenai biaya di akhir uji coba.
- ③ Penawaran tidak menyatakan periode uji coba dan pengguna mungkin tidak mengetahui durasi akses gratis yang mereka dapatkan ke konten langganan.
- ④ Penawaran seharusnya dilokalkan dalam bahasa yang sama dengan yang digunakan pada persyaratan dan ketentuan sehingga pengguna dapat memahami keseluruhan penawaran.

## Pengelolaan & Pembatalan Langganan

Sebagai developer, Anda harus memastikan bahwa aplikasi Anda mengungkapkan dengan jelas bagaimana pengguna dapat mengelola atau membatalkan langganannya.

Anda wajib memberi tahu pengguna jika ada perubahan apa pun terhadap kebijakan langganan, pembatalan, dan pengembalian dana Anda, serta memastikan bahwa kebijakan tersebut mematuhi hukum yang berlaku.

## Iklan

Kami tidak mengizinkan aplikasi yang berisi iklan menipu atau mengganggu. Iklan hanya boleh ditampilkan dalam aplikasi yang menayangkannya. Kami menganggap iklan yang ditayangkan di aplikasi Anda sebagai bagian dari aplikasi Anda. Iklan yang ditampilkan di aplikasi Anda harus mematuhi semua kebijakan kami. Untuk mengetahui kebijakan terkait iklan perjudian, klik [di sini](#).

## Penggunaan Data Lokasi untuk Iklan

Aplikasi yang memperluas penggunaan data lokasi perangkat berbasis izin untuk menayangkan iklan tunduk pada kebijakan [Informasi Pribadi dan Sensitif](#), serta harus mematuhi persyaratan berikut:

- Penggunaan atau pengumpulan data lokasi perangkat berbasis izin untuk tujuan periklanan harus jelas bagi pengguna dan didokumentasikan dalam kebijakan privasi wajib aplikasi, termasuk penautan ke setiap kebijakan privasi jaringan iklan relevan yang membahas penggunaan data lokasi.

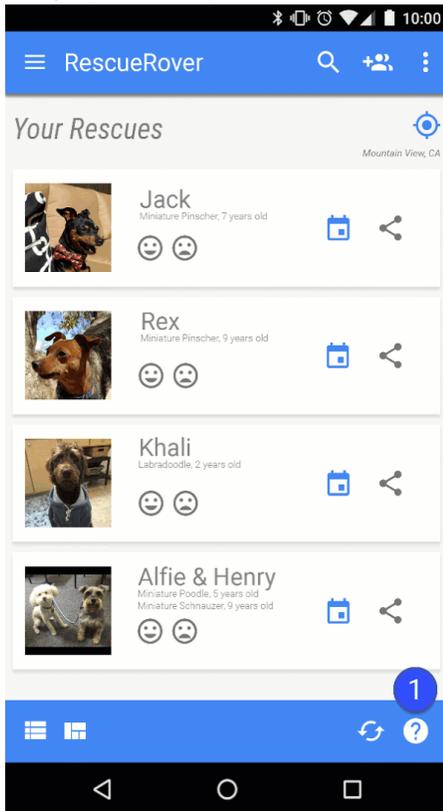
- Sesuai dengan persyaratan [Izin Akses Lokasi](#), izin akses lokasi hanya boleh diminta untuk mengimplementasikan fitur atau layanan saat ini dalam aplikasi Anda, dan tidak boleh meminta izin akses lokasi perangkat semata-mata untuk penggunaan iklan.

## Iklan yang Menipu

Iklan dilarang menyimulasikan atau meniru antarmuka pengguna aplikasi, atau elemen notifikasi dan peringatan sistem operasi apa pun. Pengguna harus bisa mengetahui dengan jelas aplikasi mana yang menayangkan iklan.

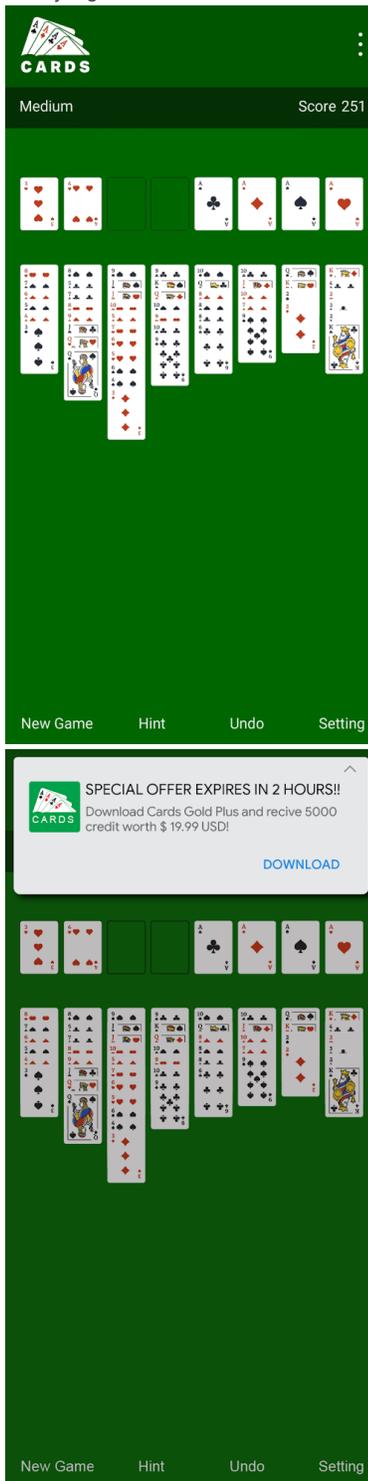
Berikut beberapa contoh pelanggaran umum:

- Iklan yang meniru UI aplikasi:



- ① Ikon tanda tanya dalam aplikasi ini adalah iklan yang mengarahkan pengguna ke halaman landing eksternal.

- Iklan yang meniru notifikasi sistem:



Contoh di atas menunjukkan iklan yang meniru berbagai notifikasi sistem.

## Monetisasi Layar Kunci

Aplikasi tidak boleh menampilkan iklan atau fitur yang memonetisasi layar perangkat yang dikunci, kecuali tujuan eksklusifnya adalah sebagai layar kunci.

## Iklan yang Mengganggu

Iklan yang mengganggu adalah iklan yang ditampilkan kepada pengguna dengan cara yang tidak diharapkan, yang dapat mengakibatkan klik yang tidak disengaja, atau menghalangi maupun mengganggu kegunaan fungsi perangkat.

Aplikasi Anda tidak boleh memaksa pengguna agar mengklik iklan atau mengirimkan informasi pribadi untuk tujuan periklanan sebelum mereka dapat sepenuhnya menggunakan aplikasi. Iklan interstitial hanya boleh ditampilkan dalam

aplikasi yang menayangkannya. Jika aplikasi Anda menampilkan iklan interstitial atau iklan lain yang mengganggu penggunaan normal, iklan tersebut harus dapat ditutup dengan mudah tanpa konsekuensi.

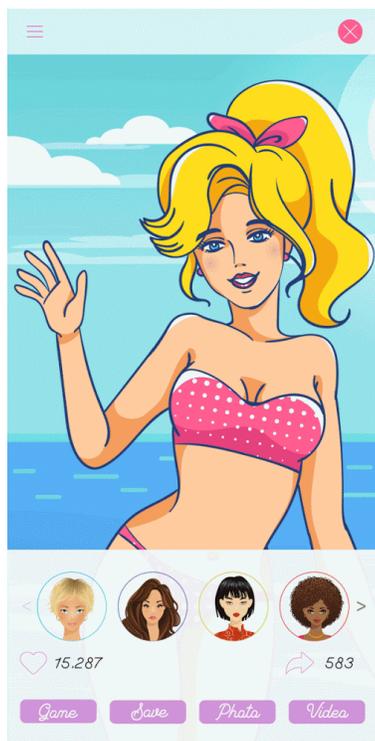
Berikut beberapa contoh pelanggaran umum:

- Iklan yang memenuhi layar atau mengganggu penggunaan normal dan tidak memberikan cara yang jelas untuk menutup iklan:

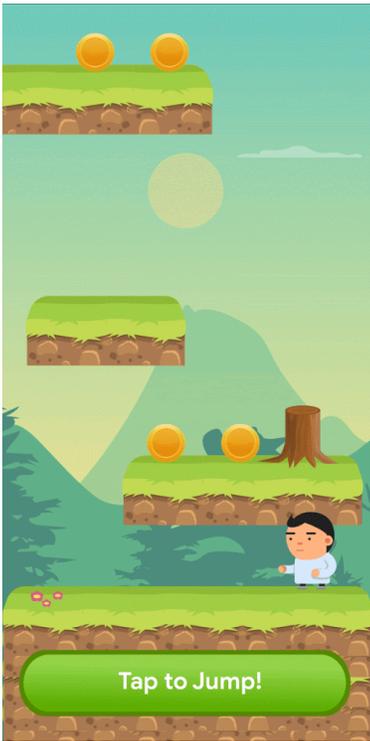


① Iklan ini tidak memiliki tombol tutup.

- Iklan yang menggunakan tombol tutup palsu untuk mengelabui pengguna agar mengkliknya, atau iklan yang didesain agar muncul tiba-tiba di area yang biasa diketuk pengguna untuk menggunakan fungsi lain aplikasi.



Iklan yang menggunakan tombol tutup palsu



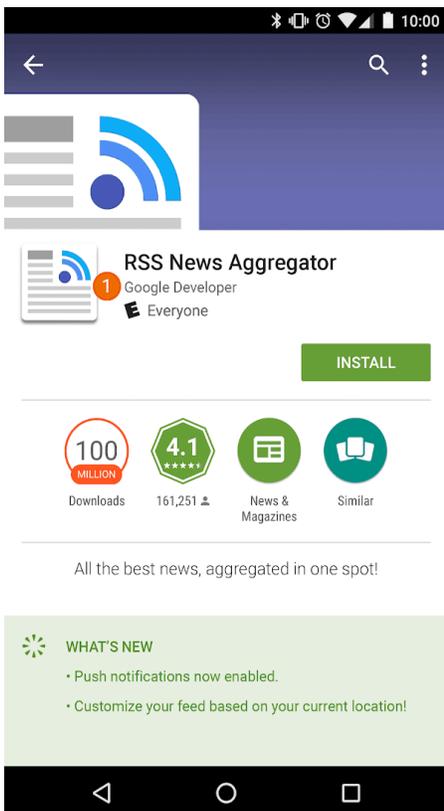
Iklan yang muncul tiba-tiba di area yang biasa diketuk pengguna untuk menggunakan fungsi dalam aplikasi

## Mengganggu Aplikasi, Iklan Pihak Ketiga, atau Fungsi Perangkat

Iklan yang terkait dengan aplikasi Anda tidak boleh mengganggu aplikasi, iklan lain, atau pengoperasian perangkat, termasuk port dan tombol perangkat atau sistem. Hal ini mencakup overlay, fungsi pengiring, dan unit iklan widget. Iklan hanya boleh ditampilkan dalam aplikasi yang menayangkannya.

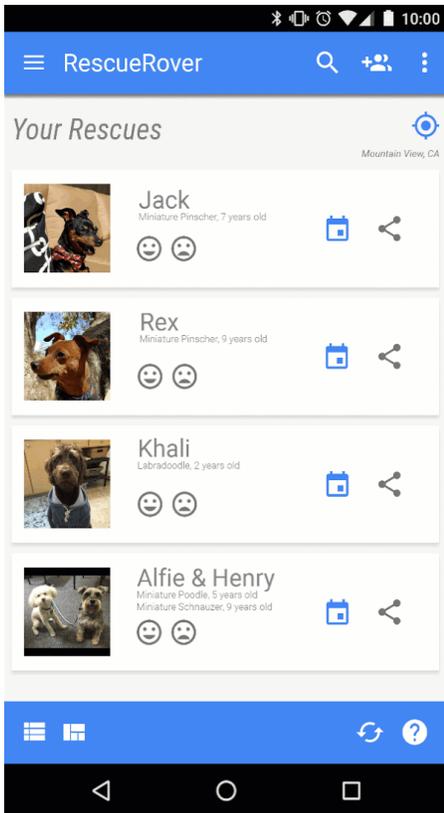
Berikut beberapa contoh pelanggaran umum:

- Iklan yang ditampilkan di luar aplikasi yang menayangkannya:



Deskripsi: Pengguna menavigasi ke layar utama dari aplikasi ini, dan tiba-tiba iklan muncul di layar utama.

- Iklan yang dipicu oleh tombol beranda atau fitur lain yang secara eksplisit dirancang untuk keluar dari aplikasi:



Deskripsi: Pengguna berupaya keluar dari aplikasi dan membuka layar utama, tetapi alurnya terganggu oleh iklan.

## Iklan yang Tidak Pantas

Iklan yang ditampilkan dalam aplikasi Anda harus pantas untuk audiens aplikasi, meskipun kontennya sendiri sudah mematuhi kebijakan kami.

Berikut adalah contoh pelanggaran umum:



- ① Iklan ini tidak pantas (Remaja) untuk target audiens aplikasi (7+)
- ② Iklan ini tidak pantas (Dewasa) untuk target audiens aplikasi (12+)

## Penggunaan ID Iklan Android

Layanan Google Play versi 4.0 memperkenalkan API dan ID baru untuk digunakan oleh penyedia periklanan dan analisis. Persyaratan untuk penggunaan ID ini dijelaskan di bawah.

- **Penggunaan.** ID iklan Android hanya boleh digunakan untuk periklanan dan analisis pengguna. Status setelah “Memilih tidak ikut dari Periklanan Menurut Minat” atau “Memilih tidak ikut dari Personalisasi Iklan” harus diverifikasi setiap kali ID diakses.
- **Keterkaitan dengan informasi identitas pribadi atau ID lainnya**
  - Penggunaan iklan: ID iklan tidak boleh dihubungkan dengan ID perangkat tetap (misalnya: SSAID, alamat MAC, IMEI, dsb.) untuk tujuan periklanan apa pun. ID iklan hanya boleh dihubungkan dengan informasi identitas pribadi melalui izin eksplisit dari pengguna.
  - Penggunaan analisis: ID iklan hanya boleh dihubungkan dengan informasi identitas pribadi atau dikaitkan dengan ID perangkat tetap (misalnya: SSAID, alamat MAC, IMEI, dsb.) melalui izin eksplisit dari pengguna.
- **Menghormati pilihan pengguna.** Apabila reset dilakukan, ID iklan baru tidak boleh dikaitkan ke ID iklan sebelumnya atau data yang berasal dari ID iklan sebelumnya tanpa persetujuan eksplisit dari pengguna. Selain itu, Anda harus mematuhi setelah “Memilih tidak ikut dari Periklanan Menurut Minat” atau “Memilih tidak ikut dari Personalisasi Iklan” pengguna. Jika pengguna telah mengaktifkan setelah ini, Anda tidak dapat menggunakan ID iklan tersebut untuk membuat profil pengguna demi tujuan periklanan, atau untuk menargetkan pengguna dengan periklanan hasil personalisasi. Aktivitas yang diperbolehkan meliputi pengiklanan kontekstual, pembatasan frekuensi, tracking konversi, pelaporan dan keamanan, serta deteksi penipuan.
- **Transparansi kepada pengguna.** Pengumpulan dan penggunaan ID iklan dan komitmen terhadap persyaratan ini harus diungkapkan kepada pengguna dalam pemberitahuan privasi yang memadai menurut hukum. Untuk mempelajari standar privasi kami lebih lanjut, tinjau kebijakan [Data Pengguna](#).
- **Mematuhi persyaratan penggunaan.** ID iklan hanya dapat digunakan sesuai persyaratan ini, termasuk oleh pihak mana pun yang dapat Anda ajak berbagi dalam aktivitas bisnis Anda. Semua aplikasi yang diupload atau dipublikasikan ke Google Play harus menggunakan ID iklan (jika tersedia di perangkat) sebagai pengganti ID perangkat lain untuk tujuan periklanan apa pun.

## Program Iklan Keluarga

Jika Anda menayangkan iklan dalam aplikasi, dan satu-satunya target audiens Anda adalah anak-anak seperti yang dijelaskan dalam [Kebijakan Keluarga](#), Anda harus menggunakan SDK iklan tersertifikasi mandiri sehubungan dengan kepatuhan terhadap kebijakan Google Play, termasuk persyaratan sertifikasi SDK Iklan di bawah. Jika target audiens aplikasi Anda mencakup anak-anak dan pengguna dewasa, Anda harus menerapkan langkah-langkah penyaringan berdasarkan usia dan memastikan bahwa iklan yang ditayangkan kepada anak-anak secara eksklusif berasal dari salah satu SDK iklan tersertifikasi mandiri ini. Aplikasi dalam program Didesain untuk Keluarga diwajibkan untuk hanya menggunakan SDK iklan tersertifikasi mandiri.

Penggunaan SDK iklan tersertifikasi Google Play hanya diwajibkan jika Anda menggunakan SDK iklan untuk menayangkan iklan kepada anak-anak. Hal-hal berikut diizinkan tanpa sertifikasi mandiri SDK iklan dengan Google Play, tetapi Anda tetap bertanggung jawab untuk memastikan bahwa praktik pengumpulan data dan konten iklan Anda mematuhi [Kebijakan Data Pengguna](#) dan [Kebijakan Keluarga](#) Play:

- Iklan Internal, yang dengannya Anda menggunakan SDK untuk mengelola promosi silang aplikasi Anda atau merchandising dan media lain yang dimiliki
- Membuat penawaran langsung dengan pengiklan, yang dengannya Anda menggunakan SDK untuk pengelolaan inventaris

### Persyaratan Sertifikasi SDK Iklan

- Mendefinisikan apa yang dimaksud dengan konten dan perilaku iklan yang tidak pantas, dan melarang keduanya dalam persyaratan atau kebijakan SDK iklan. Definisi tersebut harus mematuhi Kebijakan Program Developer Google Play.
- Membuat metode untuk memberikan rating pada materi iklan Anda berdasarkan kelompok sesuai usia. Kelompok sesuai usia setidaknya harus mencakup kelompok untuk Semua Orang dan Dewasa. Metodologi pemberian rating harus selaras dengan metodologi yang disediakan oleh Google untuk SDK setelah formulir minat di bawah diisi.
- Mengizinkan penayang, berdasarkan permintaan atau aplikasi, untuk meminta perlakuan untuk anak-anak dalam penayangan iklan. Perlakuan tersebut harus mematuhi hukum dan peraturan yang berlaku, seperti [Children's Online Privacy and Protection Act \(COPPA\) Amerika Serikat](#) dan [General Data Protection Regulation \(GDPR\) Uni Eropa](#). Google Play mewajibkan SDK iklan menonaktifkan iklan yang dipersonalisasi, periklanan menurut minat, dan pemasaran ulang sebagai bagian dari perlakuan untuk anak-anak.

- Mengizinkan penayang untuk memilih format iklan yang mematuhi [kebijakan Iklan Keluarga dan Monetisasi Play](#), serta memenuhi persyaratan [Program Disetujui Pengajar](#).
- Memastikan bahwa ketika bidding real-time digunakan untuk menayangkan iklan kepada anak-anak, materinya telah ditinjau dan indikator privasi telah disebarkan kepada bidder.
- Memberikan informasi yang memadai kepada Google, seperti informasi yang ditunjukkan dalam [formulir minat](#) di bawah, untuk memverifikasi kepatuhan SDK iklan terhadap semua persyaratan sertifikasi, lalu merespons setiap permintaan informasi selanjutnya secara tepat waktu.

*Catatan: SDK iklan harus mendukung penayangan iklan yang mematuhi semua hukum dan peraturan yang relevan terkait anak-anak, yang mungkin berlaku bagi penayangannya.*

Persyaratan mediasi untuk platform penayangan saat menayangkan iklan kepada anak-anak:

- Hanya menggunakan SDK iklan tersertifikasi Play atau mengimplementasikan perlindungan yang diperlukan untuk memastikan bahwa semua iklan yang ditayangkan dari mediasi telah mematuhi persyaratan ini; dan
- Meneruskan informasi yang diperlukan ke platform mediasi untuk menunjukkan rating konten iklan dan perlakuan untuk anak-anak yang berlaku.

Developer dapat melihat [daftar SDK iklan tersertifikasi mandiri](#) di sini.

Selain itu, developer juga dapat membagikan [formulir minat](#) ini dengan SDK iklan yang ingin mendapatkan sertifikasi mandiri.

## Listingan Play Store dan Promosi

Promosi dan visibilitas aplikasi Anda sangat memengaruhi kualitas app store. Jangan mengisi listingan Play Store dengan spam, promosi berkualitas rendah, dan upaya lain yang dibuat-buat untuk meningkatkan visibilitas aplikasi di Google Play.

## Promosi Aplikasi

Kami tidak mengizinkan aplikasi yang terlibat langsung maupun tidak langsung dalam atau mendapatkan keuntungan dari praktik promosi yang menipu atau merugikan pengguna atau ekosistem developer. Termasuk aplikasi yang terlibat dalam perilaku berikut:

- Menggunakan iklan menipu di situs web, aplikasi, atau properti lainnya, termasuk notifikasi yang mirip dengan notifikasi dan peringatan sistem.
- Taktik penginstalan atau promosi yang mengarahkan pengguna ke Google Play atau mendownload aplikasi tanpa disadari oleh pengguna.
- Promosi yang tidak diminta melalui layanan SMS.

Anda bertanggung jawab untuk memastikan bahwa jaringan iklan atau afiliasi apa pun yang terkait dengan aplikasi Anda tunduk pada kebijakan ini dan tidak menerapkan praktik promosi apa pun yang dilarang.

## Metadata

Kami melarang aplikasi dengan metadata yang menyesatkan, salah format, non-deskriptif, tidak relevan, berlebihan, atau tidak pantas, termasuk tetapi tidak terbatas pada deskripsi aplikasi, nama developer, judul, ikon, screenshot, dan gambar promosi. Developer harus memberikan deskripsi aplikasi yang jelas dan ditulis dengan baik. Kami juga melarang testimoni pengguna anonim atau tanpa atribut dalam deskripsi aplikasi.

Selain persyaratan yang disebutkan di sini, Kebijakan Developer Play tertentu mungkin mengharuskan Anda untuk memberikan informasi metadata tambahan.

**Berikut beberapa contoh pelanggaran umum:**

The best way to find a new furry friend!

RescueRover lets you use your Android device to search for rescue dogs.

1

See how much our users love us:

"It was easy to find the right dog for me and my family!"

2

It's the #1 app after Pet Rescue Saga, but in real life!

50% cooler and 100% faster than FidoFinder

3

You can see black dogs, brown dogs, white dogs, big dogs, medium dogs, small dogs, dog leashes, dog training books, dog bowls, dog toys, dog accessories. dog, dogs, rescue, shelter, animal, pet, pets, adopt, foster, puppy, puppies, dogs including:

- 1) golden retriever
- 2) labradoodle
- 3) poodle
- 4) chihuahua
- 5) akita
- 6) pug
- 7) rottweiler



- ① Testimoni Pengguna Anonim atau Tanpa Atribut
- ② Perbandingan data aplikasi atau brand
- ③ Blok kata dan daftar kata vertikal/horizontal

Berikut beberapa contoh teks, gambar, atau video yang tidak pantas disertakan dalam listingan Anda:

- Gambar atau video dengan konten yang menjerus secara seksual. Hindari gambar menjerus yang di dalamnya memuat payudara, bokong, alat kelamin, ataupun bagian tubuh atau konten seksual lainnya, baik yang berupa ilustrasi maupun gambar asli.
- Penggunaan bahasa yang tidak sopan, vulgar, atau bahasa lain yang tidak pantas untuk audiens umum di listingan Play Store aplikasi Anda.
- Unsur kekerasan yang digambarkan secara mencolok dalam ikon aplikasi, gambar, atau video promosi.
- Penggambaran penggunaan obat-obatan terlarang. Konten EDSA (Edukasi, Dokumenter, Ilmiah, atau Artistik) juga harus sesuai untuk seluruh audiens dalam listingan Play Store.

Berikut beberapa praktik terbaik:

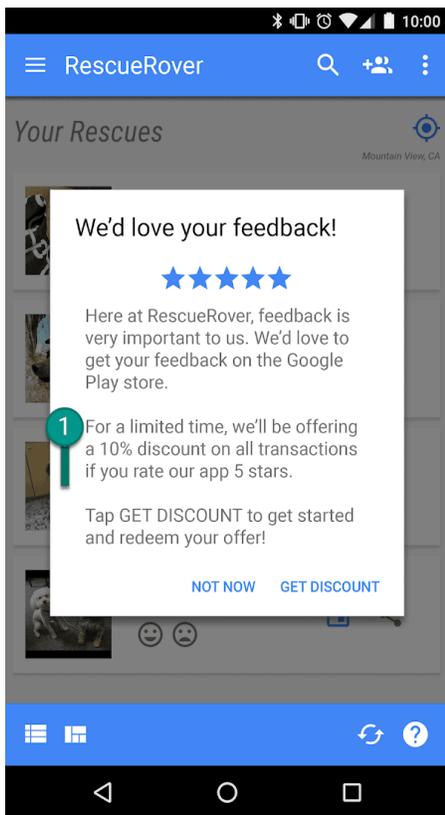
- Soroti keunggulan aplikasi Anda. Bagikan fakta menarik dan unik tentang aplikasi Anda agar pengguna memahami keistimewaannya.
- Pastikan judul dan deskripsi aplikasi Anda menggambarkan fungsi aplikasi secara akurat.
- Hindari penggunaan kata kunci maupun referensi berulang atau tidak berhubungan.
- Buat deskripsi aplikasi yang ringkas dan lugas. Deskripsi yang lebih singkat cenderung memberikan pengalaman pengguna yang lebih baik, terutama pada perangkat dengan layar lebih kecil. Deskripsi yang terlalu panjang, terlalu detail, salah format, atau diulang-ulang secara berlebihan dapat melanggar kebijakan ini.
- Perlu diingat bahwa listingan Anda harus sesuai untuk audiens umum. Hindari penggunaan teks, gambar, atau video yang tidak pantas di listingan Anda dan patuhi panduan di atas.

## Rating, Ulasan, dan Instal dari Pengguna

Developer tidak boleh berupaya memanipulasi penempatan aplikasi apa pun di Google Play. Hal ini termasuk, tetapi tidak terbatas pada, menaikkan rating produk, ulasan, atau jumlah instal secara tidak sah, seperti instal, ulasan, dan rating palsu atau yang disebabkan adanya insentif.

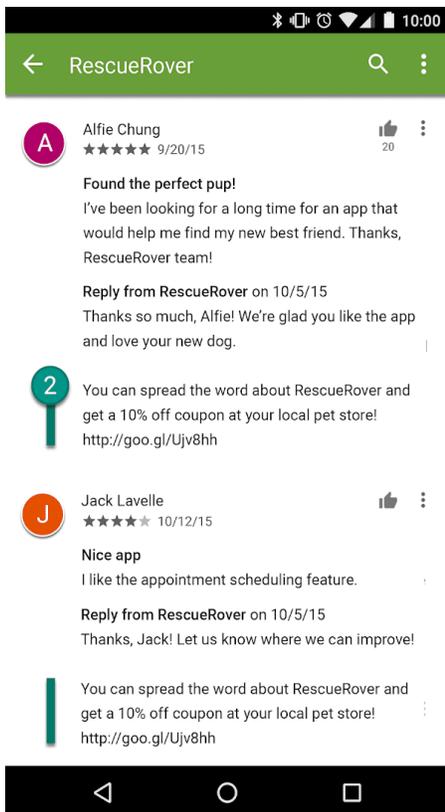
Berikut beberapa contoh pelanggaran umum:

- Meminta pengguna untuk menilai aplikasi Anda sembari menawarkan insentif:



① Notifikasi ini menawarkan diskon kepada pengguna asalkan mereka memberikan nilai yang tinggi.

- Berulang kali mengirimkan rating untuk memengaruhi penempatan aplikasi di Google Play.
- Mengirimkan atau mendorong pengguna untuk mengirimkan ulasan yang berisi konten yang tidak pantas, termasuk afiliasi, kupon, kode game, alamat email, atau link ke situs maupun aplikasi lain:



② Ulasan ini mendorong pengguna untuk mempromosikan aplikasi RescueRover dengan menawarkan kupon.

Rating dan ulasan adalah tolok ukur kualitas aplikasi. Pengguna berharap nilai dan ulasan tersebut autentik dan relevan. Berikut beberapa praktik terbaik ketika menanggapi ulasan pengguna:

- Buat balasan Anda tetap fokus pada masalah dalam komentar pengguna dan jangan meminta nilai yang lebih tinggi.
- Sertakan referensi ke sumber daya yang bermanfaat seperti alamat dukungan atau halaman FAQ.

## Rating Konten

Rating konten di Google Play disediakan oleh International Age Rating Coalition (IARC) dan didesain untuk membantu developer memberitahukan rating konten yang relevan secara lokal kepada pengguna. Otoritas IARC regional memiliki pedoman yang digunakan untuk menentukan tingkat kedewasaan konten dalam aplikasi. Kami melarang aplikasi yang tidak memiliki rating konten di Google Play.

## Penggunaan rating konten

Rating konten digunakan untuk memberi tahu konsumen, terutama orang tua, tentang potensi konten tidak pantas yang ada dalam aplikasi. Rating konten juga membantu untuk memfilter atau memblokir konten Anda di wilayah tertentu atau kepada pengguna tertentu jika diwajibkan oleh hukum, dan menentukan kelayakan aplikasi Anda untuk program developer khusus.

## Penetapan rating konten

Untuk menerima rating konten, Anda harus mengisi [kuesioner rating di Konsol Play](#) yang berisi pertanyaan tentang sifat konten aplikasi Anda. Rating konten aplikasi akan ditetapkan oleh beberapa otoritas rating berdasarkan respons kuesioner Anda. Pernyataan yang tidak benar tentang konten aplikasi dapat menyebabkan aplikasi Anda dihapus atau ditangguhkan. Oleh karena itu, Anda harus memberikan respons yang akurat saat mengisi kuesioner rating konten.

Agar aplikasi tidak dicantumkan sebagai "Belum diberi rating", Anda harus menyelesaikan kuesioner rating konten untuk setiap aplikasi baru yang dikirim ke Konsol Play, serta untuk semua aplikasi yang sudah ada dan aktif di Google Play.

Jika membuat perubahan pada fitur atau konten aplikasi yang memengaruhi respons kuesioner rating, Anda harus mengirim kuesioner rating konten baru di Konsol Play.

Buka [Pusat Bantuan](#) untuk mendapatkan informasi selengkapnya tentang berbagai [otoritas rating](#) dan cara menyelesaikan kuesioner rating konten.

## Pengajuan banding untuk rating

Jika tidak setuju dengan rating yang ditetapkan pada aplikasi, Anda dapat langsung mengajukan banding kepada otoritas rating IARC menggunakan link yang disediakan di email sertifikat.

## Berita

Aplikasi yang menyatakan dirinya sebagai aplikasi "Berita" di Google Play harus memenuhi semua persyaratan berikut.

Aplikasi berita yang mewajibkan pengguna membeli langganan harus menyediakan pratinjau konten untuk pengguna sebelum mereka membelinya.

Aplikasi berita HARUS:

- memberikan informasi kepemilikan tentang penerbit berita dan kontributornya, termasuk, tetapi tidak terbatas pada, situs resmi untuk berita yang dipublikasikan di aplikasi Anda, informasi kontak yang valid dan dapat diverifikasi, serta penerbit asli dari setiap artikel, dan
- memiliki situs atau halaman dalam aplikasi yang memberikan informasi kontak yang valid terkait penerbit berita.

Aplikasi Berita TIDAK BOLEH:

- berisi kesalahan ejaan dan/atau tata bahasa yang signifikan,
- hanya berisi konten statis (mis., konten yang dipublikasikan beberapa bulan), dan
- memiliki tujuan utama sebagai marketing afiliasi atau untuk menghasilkan pendapatan dari iklan.

Aplikasi berita yang menggabungkan konten dari berbagai sumber publikasi harus transparan tentang sumber publikasi konten dalam aplikasi dan setiap sumber harus memenuhi persyaratan kebijakan Berita.

## Spam dan Fungsi Minimum

Setidaknya, aplikasi harus memberikan fungsi dasar dan pengalaman yang layak kepada pengguna. Aplikasi yang tidak bekerja, yang menunjukkan perilaku lain tanpa memberikan pengalaman pengguna yang fungsional, atau yang hanya

menjadi spam bagi pengguna atau Google Play, bukanlah aplikasi yang pantas dimasukkan ke katalog.

## Spam

Kami tidak mengizinkan aplikasi yang mengirim spam kepada pengguna atau Google Play, seperti aplikasi yang mengirim pesan kepada pengguna tanpa diminta, atau yang bersifat pengulangan atau berkualitas rendah.

## Spam Pesan

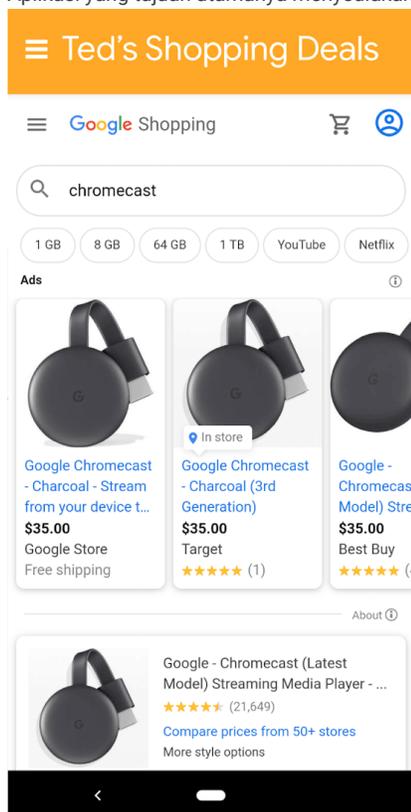
Kami tidak mengizinkan aplikasi yang mengirimkan SMS, email, atau pesan lain atas nama pengguna, tanpa memberi pengguna cara mengonfirmasi konten dan penerima yang dimaksud.

## Spam Webview dan Afiliasi

Kami tidak mengizinkan aplikasi yang tujuan utamanya adalah mengarahkan traffic afiliasi ke suatu situs, atau menyediakan webview situs tanpa izin dari pemilik maupun administratornya.

Berikut beberapa contoh pelanggaran umum:

- Aplikasi yang tujuan utamanya mengarahkan traffic rujukan ke suatu situs untuk mendapatkan kredit pendaftaran pengguna atau pembelian di situs tersebut.
- Aplikasi yang tujuan utamanya menyediakan webview situs tanpa izin:



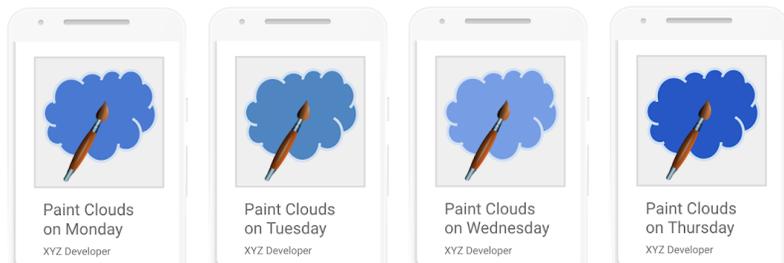
Aplikasi ini bernama "Ted's Shopping Deals" (Promo Belanja Ted) dan hanya menyediakan webview Google Shopping.

## Konten Berulang

Kami tidak mengizinkan aplikasi yang hanya memberikan pengalaman yang sama dengan aplikasi lain yang sudah ada di Google Play. Aplikasi harus memberikan nilai kepada pengguna melalui pembuatan konten atau layanan yang unik.

Berikut beberapa contoh pelanggaran umum:

- Menyalin konten dari aplikasi lain tanpa menambahkan konten atau nilai asli apa pun.
- Membuat beberapa aplikasi dengan fungsi, konten, dan pengalaman pengguna yang sangat mirip. Jika setiap aplikasi tersebut hanya memiliki sedikit konten, sebaiknya developer cukup membuat satu aplikasi yang menggabungkan semua konten itu.



## Dibuat untuk Iklan

Kami tidak mengizinkan aplikasi yang tujuan utamanya adalah menayangkan iklan.

Berikut beberapa contoh pelanggaran umum:

- Aplikasi yang selalu menayangkan iklan interstitial setelah pengguna melakukan tindakan, termasuk tetapi tidak terbatas pada mengklik, menggeser, dll.

## Fungsi Minimum

Pastikan aplikasi Anda memberikan pengalaman pengguna yang stabil, menarik, dan responsif.

Berikut beberapa contoh pelanggaran umum:

- Aplikasi yang didesain tanpa fungsi atau tidak melakukan apa pun

## Fungsi Rusak

Kami tidak mengizinkan aplikasi yang tidak bekerja, menutup secara paksa, tiba-tiba berhenti beroperasi, atau berfungsi secara tidak normal.

Berikut beberapa contoh pelanggaran umum:

- Aplikasi yang **tidak dapat diinstal**
- Aplikasi yang dapat diinstal, tetapi **tidak dapat memuat**
- Aplikasi yang dapat memuat, tetapi **tidak responsif**

## Program Lain

Selain mematuhi kebijakan konten yang ditetapkan pada bagian lain dalam Pusat Kebijakan ini, aplikasi yang dirancang untuk pengalaman Android lain dan didistribusikan melalui Google Play juga dapat tunduk terhadap persyaratan kebijakan khusus program. Pastikan Anda memeriksa daftar di bawah untuk menentukan apakah ada kebijakan yang berlaku untuk aplikasi Anda.

## Aplikasi Instan Android

Kami membuat Aplikasi Instan Android dengan tujuan untuk memberikan pengalaman pengguna yang menyenangkan dan tanpa gangguan, tetapi tetap mematuhi standar tertinggi terkait privasi dan keamanan. Kebijakan kami didesain untuk mendukung tujuan tersebut.

Developer yang memilih untuk mendistribusikan Aplikasi Instan Android melalui Google Play harus mematuhi kebijakan berikut, di samping semua [Kebijakan Program Developer Google Play](#) lainnya.

## Identitas

Untuk aplikasi instan yang menyertakan fungsi login, developer harus mengintegrasikan fitur [Smart Lock untuk Sandi](#).

## Dukungan Link

Developer Aplikasi Instan Android harus mendukung link untuk aplikasi lain dengan benar. Jika aplikasi instan atau aplikasi terinstal milik developer memuat link yang kemungkinan mengarah ke aplikasi instan, developer harus mengarahkan pengguna ke aplikasi instan tersebut, bukan membuka link di [WebView](#), misalnya.

## Spesifikasi Teknis

Developer harus mematuhi persyaratan dan spesifikasi teknis Aplikasi Instan Android yang ditetapkan oleh Google, yang dapat berubah dari waktu ke waktu, termasuk yang tercantum dalam [dokumentasi publik kami](#).

## Menawarkan Pengeinstalan Aplikasi

Aplikasi instan dapat menawarkan aplikasi yang dapat diinstal kepada pengguna, tetapi hal ini tidak boleh menjadi tujuan utama aplikasi instan. Saat menawarkan pengeinstalan, developer:

- Harus menggunakan [ikon "dapatkan aplikasi" Desain Material](#) dan label "instal" untuk tombol pengeinstalan.
- Tidak boleh memiliki lebih dari 2-3 perintah pengeinstalan implisit di aplikasi instan.
- Tidak menggunakan banner atau teknik mirip iklan lainnya, untuk menampilkan permintaan pengeinstalan kepada pengguna.

Detail aplikasi instan dan pedoman UX lainnya dapat ditemukan dalam [Praktik Terbaik untuk Pengalaman Pengguna](#).

## Mengubah Status Perangkat

Aplikasi instan tidak boleh melakukan perubahan terhadap perangkat pengguna yang bertahan lebih lama daripada sesi aplikasi instan. Misalnya, aplikasi instan mungkin tidak boleh mengubah wallpaper pengguna atau membuat widget layar utama.

## Visibilitas Aplikasi

Developer harus memastikan bahwa aplikasi instan terlihat oleh pengguna, sehingga pengguna selalu mengetahui bahwa aplikasi instan sedang berjalan di perangkatnya.

## ID Perangkat

Aplikasi instan dilarang mengakses ID perangkat sehingga (1) tetap sama setelah aplikasi instan berhenti berjalan dan (2) tidak dapat direset oleh pengguna. Contoh mencakup, tetapi tidak terbatas pada:

- Seri Build
- Alamat MAC dari chip jaringan apa pun
- IMEI, IMSI

Aplikasi instan dapat mengakses nomor telepon jika diperoleh menggunakan izin waktu proses. Developer tidak boleh mencoba mengenali pengguna menggunakan ID ini atau dengan cara lainnya.

## Traffic jaringan

Traffic jaringan dari dalam aplikasi instan harus dienkripsi menggunakan protokol TLS, seperti HTTPS.

## Keluarga

Google Play menawarkan platform yang kaya bagi developer untuk menampilkan konten berkualitas tinggi dan sesuai untuk seluruh anggota keluarga dari berbagai kelompok usia. Sebelum mengirimkan aplikasi ke program Didesain untuk Keluarga atau mengirimkan aplikasi yang menargetkan anak-anak ke Google Play Store, Anda bertanggung jawab untuk memastikan bahwa aplikasi Anda sesuai untuk anak-anak dan mematuhi semua hukum yang relevan.

Pelajari proses keluarga dan tinjau checklist interaktif di [Academy for App Success](#).

## Mendesain Aplikasi untuk Anak-Anak dan Keluarga

Penggunaan teknologi sebagai alat untuk meningkatkan kualitas hidup keluarga terus berkembang, dan para orang tua kini mencari konten yang berkualitas tinggi dan aman untuk diberikan kepada anak-anak mereka. Aplikasi Anda mungkin didesain khusus untuk anak-anak atau mungkin menarik perhatian mereka. Google Play ingin membantu Anda memastikan aplikasi Anda aman bagi semua pengguna, termasuk keluarga.

Kata "anak-anak" memiliki arti yang berbeda di berbagai tempat dan konteks. Sebaiknya hubungi penasihat hukum Anda untuk membantu mengetahui kewajiban dan/atau batasan berdasarkan usia yang berlaku untuk aplikasi Anda. Adalah yang paling tahu cara kerja aplikasi Anda, sehingga kami memercayai Anda untuk membantu kami memastikan aplikasi di Google Play aman bagi keluarga.

Aplikasi yang didesain secara khusus untuk anak-anak harus berpartisipasi dalam program Didesain untuk Keluarga. Jika aplikasi Anda menargetkan audiens anak-anak dan yang lebih tua, Anda tetap dapat berpartisipasi dalam program Didesain untuk Keluarga. Semua aplikasi yang ikut serta dalam program Didesain untuk Keluarga akan memenuhi syarat untuk diberi rating terkait [program Disetujui Pengajar](#), tetapi kami tidak dapat menjamin bahwa aplikasi Anda akan

disertakan dalam program Ditetujui Pengajar. Jika Anda memutuskan untuk tidak berpartisipasi dalam program Didesain untuk Keluarga, Anda tetap harus mematuhi persyaratan Kebijakan Keluarga Google Play di bawah, serta [Kebijakan Program Developer Google Play](#) dan [Perjanjian Distribusi Developer](#) lainnya.

## Persyaratan Konsol Play

### [Target Audiens dan Konten](#)

Pada bagian [Target Audiens dan Konten](#) di Konsol Google Play, Anda harus menentukan target audiens aplikasi Anda sebelum memublikasikannya, dengan memilih opsi dari daftar kelompok usia yang disediakan. Terlepas dari identifikasi yang Anda lakukan di Konsol Google Play, jika Anda memilih untuk menyertakan citra atau istilah dalam aplikasi Anda yang dapat dianggap menargetkan anak-anak, tindakan ini dapat memengaruhi penilaian Google Play terhadap target audiens yang Anda nyatakan. Google Play berhak melakukan peninjauannya sendiri atas informasi aplikasi yang Anda berikan untuk menentukan apakah target audiens yang Anda ungkapkan sudah akurat.

Jika Anda memilih target audiens yang hanya mencakup orang dewasa, tetapi Google memutuskan bahwa target ini tidak akurat karena aplikasi Anda menargetkan anak-anak dan orang dewasa, Anda akan memiliki opsi untuk menjelaskan kepada pengguna bahwa aplikasi Anda tidak menargetkan anak-anak dengan menyetujui untuk memberikan label peringatan.

Anda hanya perlu memilih lebih dari satu kelompok usia untuk target audiens aplikasi jika Anda memang mendesain aplikasi untuk pengguna dalam kelompok-kelompok usia yang dipilih tersebut dan telah memastikan bahwa aplikasi Anda sesuai untuk mereka. Misalnya, aplikasi yang didesain untuk bayi, balita, dan anak-anak PAUD hanya boleh memilih kelompok usia "5 Tahun ke Bawah" sebagai target kelompok usianya. Jika aplikasi Anda didesain untuk tingkat sekolah tertentu, pilih kelompok usia yang paling mewakili tingkat sekolah tersebut. Anda sebaiknya hanya memilih kelompok usia yang menyertakan dewasa dan anak-anak jika Anda benar-benar telah mendesain aplikasi Anda untuk semua usia.

### Memperbarui Bagian Target Audiens dan Konten

Anda dapat memperbarui informasi aplikasi Anda kapan saja di bagian Target Audiens dan Konten di Konsol Google Play. [Update aplikasi](#) diperlukan agar informasi ini dapat ditampilkan di Google Play Store. Namun, perubahan apa pun yang Anda lakukan pada bagian ini di Konsol Google Play mungkin akan ditinjau kepatuhannya terhadap kebijakan meskipun update aplikasi belum dikirim.

Kami sangat merekomendasikan agar Anda memberi tahu pengguna lama jika Anda mengubah target kelompok usia untuk aplikasi Anda dan mulai menggunakan iklan atau fitur pembelian dalam aplikasi, baik dengan menggunakan bagian "Fitur Baru" di halaman listingan Play Store aplikasi Anda maupun melalui notifikasi dalam aplikasi.

### Pernyataan Tidak Benar di Konsol Google Play

Pernyataan tidak benar terkait informasi apa pun tentang aplikasi Anda di Konsol Google Play, termasuk di bagian Target Audiens dan Konten, dapat menyebabkan aplikasi Anda dihapus atau ditangguhkan, sehingga penting untuk menyediakan informasi yang akurat.

## Persyaratan Kebijakan Keluarga

Jika salah satu target audiens untuk aplikasi Anda adalah anak-anak, Anda harus mematuhi persyaratan berikut. Kegagalan dalam memenuhi persyaratan ini dapat menyebabkan aplikasi dihapus atau ditangguhkan.

- Konten aplikasi:** Konten yang dapat diakses oleh anak-anak dalam aplikasi Anda harus sesuai untuk anak-anak.
- Jawaban Konsol Google Play:** Anda harus menjawab pertanyaan di Konsol Google Play mengenai aplikasi Anda dengan tepat, dan memperbarui jawaban tersebut untuk merefleksikan setiap perubahan pada aplikasi Anda secara akurat.
- Iklan:** Jika aplikasi menampilkan iklan kepada anak-anak atau kepada pengguna dengan usia yang tidak diketahui, Anda harus:
  - menggunakan [SDK iklan tersertifikasi Google Play](#) secara eksklusif untuk menampilkan iklan kepada pengguna tersebut;
  - memastikan iklan yang ditampilkan kepada pengguna tersebut tidak menyertakan periklanan menurut minat (iklan yang ditargetkan kepada pengguna individu dengan karakteristik tertentu berdasarkan perilaku penjelajahan mereka di internet) atau pemasaran ulang (iklan yang ditargetkan kepada pengguna individu berdasarkan interaksi sebelumnya dengan suatu aplikasi atau situs);
  - memastikan iklan yang ditampilkan kepada pengguna tersebut menayangkan konten yang sesuai untuk anak-anak;
  - memastikan iklan yang ditampilkan kepada pengguna tersebut mematuhi persyaratan format iklan Keluarga; dan
  - memastikan kepatuhan terhadap semua peraturan hukum dan standar industri yang berlaku terkait periklanan untuk anak-anak.
- Pengumpulan Data:** Anda harus mengungkapkan pengumpulan [informasi pribadi dan sensitif](#) apa pun dari anak-anak di aplikasi Anda, termasuk melalui API dan SDK yang dipanggil atau digunakan di aplikasi Anda. Informasi sensitif dari

anak-anak termasuk, tetapi tidak terbatas pada, informasi autentikasi, data mikrofon dan sensor kamera, data perangkat, ID Android, data penggunaan iklan, serta ID iklan.

5. **API dan SDK:** Anda harus memastikan bahwa aplikasi Anda mengimplementasikan setiap API dan SDK dengan benar.
  - Aplikasi yang hanya menargetkan anak-anak tidak boleh berisi API atau SDK yang tidak disetujui penggunaannya dalam layanan yang ditujukan untuk anak-anak. Ini mencakup, Login dengan Google (atau Layanan Google API apa pun yang mengakses data yang terkait dengan Akun Google), Layanan Game Google Play, dan Layanan API lainnya yang menggunakan teknologi OAuth untuk proses autentikasi dan otorisasi.
  - Aplikasi yang menargetkan audiens anak-anak dan yang lebih tua tidak boleh mengimplementasikan API atau SDK yang tidak disetujui penggunaannya dalam layanan yang ditujukan untuk anak-anak, kecuali digunakan di balik [layar verifikasi usia](#) atau diimplementasikan tanpa mengumpulkan data dari anak-anak (misalnya menyediakan Login dengan Google sebagai fitur opsional). Aplikasi yang menargetkan audiens anak-anak dan yang lebih tua tidak boleh mewajibkan pengguna untuk login atau mengakses konten aplikasi melalui API atau SDK yang tidak disetujui penggunaannya dalam layanan yang ditujukan untuk anak-anak.
6. **Kebijakan privasi:** Anda harus menyediakan link ke kebijakan privasi aplikasi Anda di halaman listingan Play Store aplikasi. Link ini harus dikelola setiap saat selama aplikasi tersedia di Store, dan harus ditautkan ke kebijakan privasi yang, di antaranya, menjelaskan pengumpulan dan penggunaan data aplikasi Anda secara akurat.
7. **Batasan khusus:**
  - Jika aplikasi Anda menggunakan Augmented Reality, Anda harus menyertakan peringatan keamanan langsung setelah peluncuran bagian AR. Peringatan harus memuat hal berikut:
    - Pesan yang sesuai tentang pentingnya pengawasan orang tua.
    - Peringatan untuk mewaspadaai adanya bahaya fisik di dunia nyata (misalnya waspada dengan keadaan sekitar Anda).
  - Aplikasi Anda tidak boleh mewajibkan penggunaan perangkat yang tidak disarankan untuk anak-anak (misalnya Daydream, Oculus).
8. **Kepatuhan Hukum:** Anda harus memastikan bahwa aplikasi Anda, termasuk setiap API atau SDK yang dipanggil atau digunakan oleh aplikasi Anda, mematuhi [Children's Online Privacy and Protection Act \(COPPA\) Amerika Serikat](#), [General Data Protection Regulation \(GDPR\) Uni Eropa](#), dan hukum atau peraturan lain yang berlaku.

Berikut beberapa contoh pelanggaran umum:

- Aplikasi yang mempromosikan permainan untuk anak-anak di listingan Play Store, tetapi konten aplikasinya hanya sesuai untuk orang dewasa.
- Aplikasi yang mengimplementasikan API dengan persyaratan layanan yang melarang penggunaannya dalam aplikasi yang ditujukan untuk anak-anak.
- Aplikasi yang menonjolkan penggunaan alkohol, tembakau, atau zat yang dikendalikan.
- Aplikasi yang menyertakan perjudian sungguhan atau simulasi.
- Aplikasi yang menyertakan konten kekerasan, sadis, atau mengerikan yang tidak pantas untuk anak-anak.
- Aplikasi yang menyediakan layanan kencan atau menawarkan konsultasi seksual maupun pernikahan.
- Aplikasi yang mencantumkan link ke situs berisi konten yang melanggar [Kebijakan Program Developer](#) Google Play.
- Aplikasi yang menampilkan iklan dewasa (misalnya konten kekerasan, konten seksual, konten perjudian) kepada anak-anak. Baca [kebijakan Iklan Keluarga dan Monetisasi](#) untuk mengetahui informasi selengkapnya tentang kebijakan Google Play terkait iklan, pembelian dalam aplikasi, dan konten komersial untuk anak-anak.

## Program Didesain untuk Keluarga

Aplikasi yang didesain secara khusus untuk anak-anak harus berpartisipasi dalam program Didesain untuk Keluarga. Jika aplikasi Anda didesain untuk segala usia, termasuk anak-anak dan keluarga, Anda juga dapat mendaftar untuk berpartisipasi dalam program tersebut.

Sebelum dapat diterima dalam program, aplikasi Anda harus memenuhi semua persyaratan Kebijakan Keluarga dan persyaratan kelayakan Didesain untuk Keluarga, di samping yang diuraikan dalam [Kebijakan Program Developer Google Play](#) dan [Perjanjian Distribusi Developer](#).

Untuk mengetahui informasi selengkapnya tentang proses pengiriman aplikasi untuk diikutsertakan dalam program tersebut, klik [di sini](#).

### Kelayakan Program

Semua aplikasi yang berpartisipasi dalam program Didesain untuk Keluarga harus memiliki konten iklan dan aplikasi yang relevan dan sesuai untuk anak-anak, dan harus mematuhi semua persyaratan di bawah. Aplikasi yang diterima dalam program Didesain untuk Keluarga harus terus mematuhi semua persyaratan program. Google Play dapat menolak, menghapus, atau menangguhkan aplikasi yang dianggap tidak pantas untuk program Didesain untuk Keluarga.

### Persyaratan Didesain untuk Keluarga

1. Aplikasi harus diberi rating sebagai ESRB Everyone atau Everyone 10+, atau yang setara.
2. Anda harus mengungkapkan elemen interaktif aplikasi secara akurat pada Kuesioner Rating Konten di Konsol Google Play, termasuk apakah:
  - pengguna dapat berinteraksi atau bertukar informasi;
  - aplikasi Anda membagikan informasi pribadi yang diberikan pengguna kepada pihak ketiga; dan
  - aplikasi Anda membagikan lokasi fisik pengguna kepada pengguna lain.
3. Jika menggunakan [Android Speech API](#), `RecognizerIntent.EXTRA_CALLING_PACKAGE` aplikasi Anda harus ditetapkan ke `PackageName`-nya.
4. Aplikasi hanya boleh menggunakan [SDK iklan tersertifikasi Google Play](#).
5. Aplikasi yang didesain secara khusus untuk anak-anak tidak dapat meminta izin akses lokasi.
6. Aplikasi harus menggunakan [Pengelola Perangkat Pendamping \(CDM\)](#) saat meminta akses Bluetooth, kecuali aplikasi Anda hanya menargetkan versi Sistem Operasi (OS) perangkat yang tidak kompatibel dengan CDM.

### Berikut beberapa contoh aplikasi umum yang tidak memenuhi syarat untuk program ini:

- Aplikasi yang diberi rating ESRB Everyone, tetapi berisi iklan untuk konten perjudian
- Aplikasi untuk orang tua atau pengasuh (misalnya pencatat aktivitas menyusui, panduan perkembangan anak)
- Panduan orang tua atau aplikasi pengelolaan perangkat yang hanya dimaksudkan untuk digunakan oleh orang tua atau pengasuh
- Aplikasi yang menggunakan ikon aplikasi atau ikon peluncur yang tidak pantas untuk anak-anak

### Kategori

Jika diterima untuk berpartisipasi dalam program Didesain untuk Keluarga, Anda dapat memilih kategori tambahan yang spesifik untuk Keluarga bagi aplikasi Anda. Berikut kategori yang tersedia untuk aplikasi yang berpartisipasi dalam program Didesain untuk Keluarga:

**Aksi & Petualangan:** Aplikasi/game yang berorientasi aksi, mulai dari game balap sederhana, petualangan dongeng, hingga aplikasi dan game lainnya yang didesain untuk memicu keseruan.

**Game Asah Otak:** Game yang mengasah kemampuan berpikir, termasuk teka-teki, game mencocokkan, kuis, dan game lainnya yang menantang memori, kecerdasan, atau logika.

**Kreativitas:** Aplikasi dan game yang memacu kreativitas, termasuk aplikasi menggambar, aplikasi mewarnai, aplikasi coding, serta aplikasi dan game lain yang memungkinkan Anda membangun sesuatu.

**Edukasi:** Aplikasi dan game yang didesain dengan masukan dari para pakar pembelajaran (misalnya pengajar, spesialis pembelajaran, peneliti) untuk mendorong proses pembelajaran, termasuk pembelajaran akademis, sosial-emosional, fisik, kreatif, serta pembelajaran terkait keterampilan hidup dasar, berpikir kritis, dan pemecahan masalah.

**Musik dan Video:** Aplikasi dan game dengan komponen musik atau video, mulai dari aplikasi simulasi instrumen hingga aplikasi yang menyediakan konten audio musikal dan video.

**Bermain Peran:** Aplikasi dan game yang memungkinkan pengguna bermain peran, misalnya berpura-pura menjadi koki, pengasuh, pangeran/putri, pemadam kebakaran, polisi, atau karakter fiksi.

## Iklan dan Monetisasi

Kebijakan di bawah berlaku bagi semua iklan dalam aplikasi Anda, termasuk iklan untuk aplikasi Anda dan aplikasi pihak ketiga, penawaran untuk pembelian dalam aplikasi, atau konten komersial lainnya (seperti penempatan produk berbayar) yang ditayangkan kepada pengguna dalam aplikasi yang tunduk pada Persyaratan Kebijakan Keluarga dan/atau Persyaratan Didesain untuk Keluarga. Semua iklan, penawaran untuk pembelian dalam aplikasi, dan konten komersial dalam aplikasi ini harus mematuhi semua hukum dan peraturan yang berlaku (termasuk peraturan mandiri atau pedoman industri yang relevan).

Google Play berhak menolak, menghapus, atau menangguhkan aplikasi jika menemukan taktik komersial yang terlalu agresif.

### Persyaratan format iklan

Iklan dan penawaran untuk pembelian dalam aplikasi dilarang memiliki konten yang bersifat menipu atau didesain sedemikian rupa untuk memperoleh klik yang tidak sengaja dari pengguna anak. Berikut adalah hal-hal yang dilarang:

- Iklan yang mengganggu, termasuk iklan yang memenuhi layar atau mengganggu penggunaan normal dan tidak memberikan cara yang jelas untuk menutup iklan (misalnya [Iklan penghalang](#))
- Iklan yang mengganggu penggunaan normal aplikasi atau alur game, yang tidak dapat ditutup setelah 5 detik. Iklan yang tidak mengganggu penggunaan normal aplikasi atau alur game boleh ditayangkan selama lebih dari 5 detik (misalnya konten video dengan iklan terintegrasi).

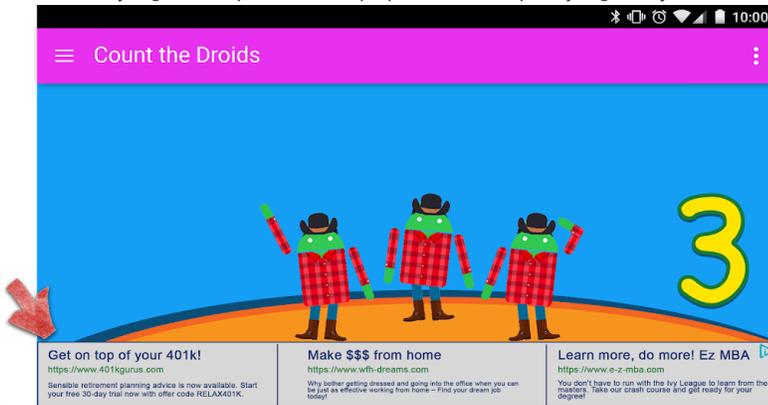
- Iklan interstitial atau penawaran untuk pembelian dalam aplikasi yang langsung muncul setelah aplikasi dibuka
- Penempatan iklan pada beberapa area di satu halaman (misalnya iklan banner yang menampilkan beberapa penawaran pada satu penempatan atau yang menampilkan lebih dari satu iklan video atau banner tidak diizinkan).
- Iklan atau penawaran untuk pembelian dalam aplikasi yang tidak dapat dibedakan dengan jelas dari konten aplikasi Anda
- Penggunaan taktik yang mengejutkan atau memanipulasi emosi untuk mengelabui pengguna agar melihat iklan atau melakukan pembelian dalam aplikasi
- Tidak membedakan antara penggunaan koin game virtual dengan uang sungguhan untuk melakukan pembelian dalam aplikasi

Berikut beberapa contoh pelanggaran umum terkait format iklan

- Iklan yang menjauh dari jari pengguna saat pengguna mencoba menutup iklan
- Iklan yang menggunakan sebagian besar ruang di layar perangkat tanpa memberikan cara yang jelas kepada pengguna untuk menutupnya, sebagaimana yang ditunjukkan dalam contoh di bawah:

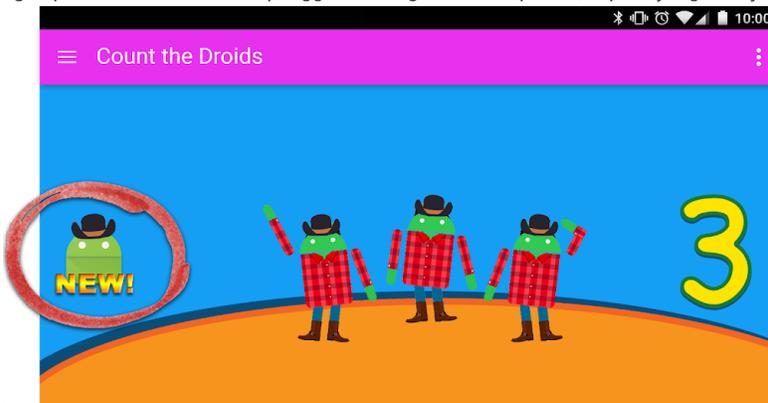


- Iklan banner yang menampilkan beberapa penawaran, seperti yang ditunjukkan dalam contoh di bawah:

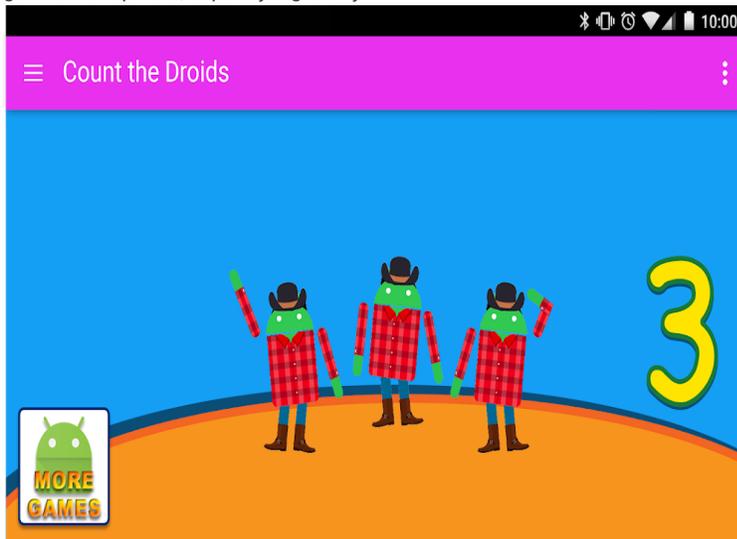


- Iklan yang dapat disalahartikan oleh pengguna sebagai konten aplikasi, seperti yang ditunjukkan dalam contoh di

bawah:



- Tombol atau iklan yang mempromosikan listingan Google Play Store Anda lainnya, tetapi tidak dapat dibedakan dengan konten aplikasi, seperti yang ditunjukkan dalam contoh di bawah:



Berikut beberapa contoh konten iklan yang tidak pantas yang tidak boleh ditampilkan kepada anak-anak.

- **Konten Media yang Tidak Pantas:** Iklan untuk acara TV, film, album musik, atau outlet media lain yang tidak sesuai untuk anak-anak.
- **Video Game yang Tidak Pantas & Software yang Dapat Didownload:** Iklan untuk software yang dapat didownload dan video game elektronik yang tidak sesuai untuk anak-anak.
- **Zat Terkontrol atau Berbahaya:** Iklan untuk alkohol, tembakau, zat terkontrol, atau zat berbahaya lainnya.
- **Perjudian:** Iklan untuk simulasi perjudian, kontes, atau promosi undian, meskipun bebas untuk diikuti.
- **Konten yang Menjurus Secara Seksual dan Konten Khusus Dewasa:** Iklan dengan konten khusus dewasa dan seksual.
- **Pacaran atau Kencan:** Iklan untuk situs kencan atau hubungan orang dewasa.
- **Konten Kekerasan:** Iklan dengan konten menjijikkan dan berisi kekerasan yang tidak sesuai untuk anak-anak.

#### SDK Iklan

Jika Anda menayangkan iklan dalam aplikasi dan anak-anak menjadi satu-satunya target audiens, Anda harus menggunakan [SDK iklan tersertifikasi Google Play](#). Jika target audiens aplikasi Anda mencakup anak-anak dan pengguna yang lebih tua, Anda harus mengimplementasikan langkah-langkah verifikasi usia, seperti [layar verifikasi usia](#), dan memastikan bahwa iklan yang ditampilkan kepada anak-anak hanya berasal dari SDK iklan tersertifikasi Google Play. Aplikasi dalam program Didesain untuk Keluarga diwajibkan untuk hanya menggunakan SDK iklan tersertifikasi mandiri.

Lihat halaman [kebijakan Program Iklan Keluarga](#) untuk mengetahui detail selengkapnya tentang persyaratan ini dan untuk melihat daftar terbaru SDK iklan yang disetujui.

Jika Anda menggunakan AdMob, lihat [Pusat Bantuan AdMob](#) untuk detail selengkapnya tentang produk tersebut.

Anda bertanggung jawab untuk memastikan bahwa aplikasi Anda memenuhi semua persyaratan terkait periklanan, pembelian dalam aplikasi, dan konten komersial. Hubungi penyedia SDK iklan Anda untuk mempelajari lebih lanjut kebijakan konten dan praktik periklanan mereka.

#### Pembelian dalam aplikasi

Google Play akan mengautentikasi ulang semua pengguna sebelum melakukan pembelian dalam aplikasi pada aplikasi yang berpartisipasi dalam program Didesain untuk Keluarga. Tujuannya adalah membantu memastikan bahwa pembelian akan disetujui oleh pihak yang bertanggung jawab secara finansial, bukan anak-anak.

## Penegakan

Menghindari pelanggaran kebijakan selalu lebih baik daripada menanganinya. Namun jika pelanggaran benar-benar telah terjadi, kami berkomitmen untuk memastikan bahwa developer mengetahui cara agar aplikasinya tetap patuh terhadap peraturan yang ada. Beri tahu kami jika Anda [menemukan pelanggaran](#) atau memiliki pertanyaan tentang [cara menangani pelanggaran](#).

## Cakupan Kebijakan

Kebijakan kami berlaku untuk konten apa pun yang ditampilkan atau ditautkan oleh aplikasi Anda, termasuk iklan apa pun yang ditampilkan kepada pengguna, dan konten apa pun buatan pengguna yang dihosting atau ditautkan oleh aplikasi. Lebih jauh lagi, kebijakan kami berlaku untuk konten apa pun dari akun developer Anda yang ditampilkan secara publik di Google Play, termasuk nama developer dan halaman landing situs developer milik Anda yang dicantumkan.

Kami melarang aplikasi yang mengizinkan pengguna menginstal aplikasi lain ke perangkatnya. Aplikasi yang memberikan akses ke game, software, atau aplikasi lain tanpa penguasaan, termasuk fitur dan pengalaman yang disediakan oleh pihak ketiga, harus memastikan bahwa semua konten yang aksesnya diberikan telah mematuhi semua [kebijakan Google Play](#) dan mungkin mendapatkan pemeriksaan kebijakan tambahan.

Istilah yang didefinisikan dan digunakan dalam kebijakan ini memiliki makna yang sama dengan yang ada dalam [Perjanjian Distribusi Developer](#) (DDA). Selain mematuhi kebijakan ini dan DDA, konten aplikasi Anda juga harus diberi rating sesuai dengan [Pedoman Rating Konten](#).

Saat menilai apakah aplikasi akan diterima atau dihapus dari Google Play, kami mempertimbangkan sejumlah faktor termasuk, tetapi tidak terbatas pada, pola perilaku yang berbahaya atau risiko penyalahgunaan yang tinggi. Kami akan mengidentifikasi risiko penyalahgunaan termasuk, tetapi tidak terbatas pada, hal-hal seperti histori pelanggaran sebelumnya, masukan pengguna, serta penggunaan brand, karakter, dan aset populer lainnya.

## Cara kerja Google Play Protect

Google Play Protect memeriksa aplikasi saat Anda menginstalnya. Layanan ini juga memindai perangkat secara berkala. Jika menemukan aplikasi yang berpotensi membahayakan, layanan ini dapat:

- Mengirimkan notifikasi kepada Anda. Untuk menghapus aplikasi, ketuk notifikasi, lalu ketuk Uninstal.
- Menonaktifkan aplikasi sampai akhirnya di-uninstal.
- Menghapus aplikasi secara otomatis. Umumnya, jika aplikasi berbahaya terdeteksi, Anda akan menerima notifikasi bahwa aplikasi tersebut telah dihapus.

## Cara kerja perlindungan dari malware

Untuk melindungi Anda dari software pihak ketiga dan URL yang berbahaya, serta masalah keamanan lainnya, Google dapat menerima informasi tentang:

- Koneksi jaringan perangkat Anda
- URL yang berpotensi membahayakan
- Sistem operasi dan aplikasi yang diinstal di perangkat Anda melalui Google Play atau sumber lainnya.

Anda dapat menerima peringatan dari Google tentang aplikasi atau URL yang mungkin tidak aman. Aplikasi atau URL tersebut dapat dihapus atau diblokir penginstalnya oleh Google jika diketahui berbahaya bagi perangkat, data, atau pengguna.

Anda dapat memilih untuk menonaktifkan beberapa perlindungan ini di setelan perangkat. Namun, Google tetap dapat menerima informasi tentang aplikasi yang diinstal melalui Google Play, dan aplikasi dari sumber lain yang diinstal di perangkat Anda juga dapat terus diperiksa untuk menemukan masalah keamanan tanpa perlu mengirim informasi ke Google.

## Cara kerja Notifikasi privasi

Google Play Protect akan memberi tahu Anda jika aplikasi dihapus dari Google Play Store karena aplikasi tersebut dapat mengakses informasi pribadi, dan Anda akan memiliki opsi untuk meng-uninstalnya.

## Proses Penegakan

Jika aplikasi Anda melanggar salah satu kebijakan kami, tindakan yang sesuai akan kami lakukan sebagaimana diuraikan di bawah. Selain itu, kami juga akan memberikan informasi yang relevan melalui email tentang tindakan yang telah kami lakukan, beserta petunjuk pengajuan banding jika Anda yakin kami telah melakukan kekeliruan.

Harap diperhatikan bahwa pemberitahuan administratif atau penghapusan mungkin tidak menunjukkan setiap pelanggaran kebijakan yang ada dalam aplikasi Anda atau katalog aplikasi yang lebih luas. Developer bertanggung jawab untuk menangani setiap masalah kebijakan yang ada dan melakukan uji tuntas tambahan untuk memastikan bahwa aplikasi mereka sepenuhnya mematuhi kebijakan. Kegagalan untuk menangani pelanggaran kebijakan dalam semua aplikasi Anda dapat mengakibatkan tindakan penegakan lebih lanjut.

Pelanggaran berulang atau serius (seperti malware, penipuan, dan aplikasi yang dapat membahayakan pengguna atau perangkat) terhadap kebijakan ini atau [Perjanjian Distribusi Developer](#) (DDA) akan mengakibatkan penghentian Akun Developer Google Play individu atau yang terkait.

## Tindakan Penegakan

Tindakan penegakan yang berbeda dapat memiliki dampak yang berbeda terhadap aplikasi Anda. Bagian berikut menjelaskan berbagai tindakan yang dapat dilakukan Google Play, serta dampaknya terhadap aplikasi dan/atau Akun Developer Google Play Anda. Informasi tersebut juga dijelaskan dalam [video ini](#).

### Penolakan

- Aplikasi baru atau update aplikasi yang dikirim untuk ditinjau tidak akan tersedia di Google Play.
- Jika update untuk aplikasi yang sudah ada ditolak, versi aplikasi yang dipublikasikan sebelum update tersebut akan tetap tersedia di Google Play.
- Anda tetap dapat mengakses instal pengguna, statistik, dan rating yang sudah ada sebelum aplikasi ditolak.
- Penolakan tidak memengaruhi status Akun Developer Google Play Anda.

Catatan: Jangan mencoba mengirim ulang aplikasi yang sudah ditolak sampai Anda memperbaiki semua pelanggaran kebijakan yang ada.

### Penghapusan

- Aplikasi, beserta semua versi sebelumnya, dihapus dari Google Play dan tidak akan tersedia lagi untuk didownload oleh pengguna.
- Apabila aplikasi dihapus, pengguna tidak dapat lagi melihat listingan Play Store, jumlah instal pengguna, statistik, dan rating untuk aplikasi tersebut. Informasi ini akan dipulihkan setelah Anda mengirimkan update yang mematuhi kebijakan untuk aplikasi yang dihapus.
- Pengguna mungkin tidak dapat melakukan pembelian dalam aplikasi, atau menggunakan fitur penagihan via Google Play dalam aplikasi hingga versi yang mematuhi kebijakan disetujui oleh Google Play.
- Penghapusan tidak akan berdampak langsung terhadap status Akun Developer Google Play Anda, tetapi penghapusan yang terjadi beberapa kali dapat mengakibatkan penangguhan akun.

Catatan: Jangan mencoba memublikasikan ulang aplikasi yang sudah dihapus sampai Anda memperbaiki semua pelanggaran kebijakan yang ada.

### Penangguhan

- Aplikasi, beserta semua versi sebelumnya, dihapus dari Google Play dan tidak akan tersedia lagi untuk didownload oleh pengguna.
- Penangguhan dapat terjadi sebagai akibat dari pelanggaran kebijakan yang berat atau berulang, serta penolakan atau penghapusan aplikasi yang terjadi berulang kali.
- Apabila aplikasi ditangguhkan, pengguna tidak dapat lagi melihat listingan Play Store, jumlah instal pengguna yang sudah ada, statistik, dan rating untuk aplikasi tersebut. Informasi ini akan dipulihkan setelah Anda mengirimkan update yang mematuhi kebijakan untuk aplikasi yang dihapus.
- Anda tidak dapat lagi menggunakan APK atau app bundle aplikasi yang ditangguhkan.
- Pengguna tidak akan bisa melakukan pembelian dalam aplikasi, atau menggunakan fitur penagihan via Google Play dalam aplikasi hingga versi yang mematuhi kebijakan disetujui oleh Google Play.
- Penangguhan dianggap sebagai teguran terhadap reputasi baik Akun Developer Google Play Anda. Teguran yang diterima berulang kali dapat mengakibatkan penghentian Akun Developer Google Play individu dan yang terkait.

Catatan: Jangan mencoba memublikasikan ulang aplikasi yang ditangguhkan sebelum Google Play menjelaskan bahwa Anda boleh melakukannya.

### Visibilitas Terbatas

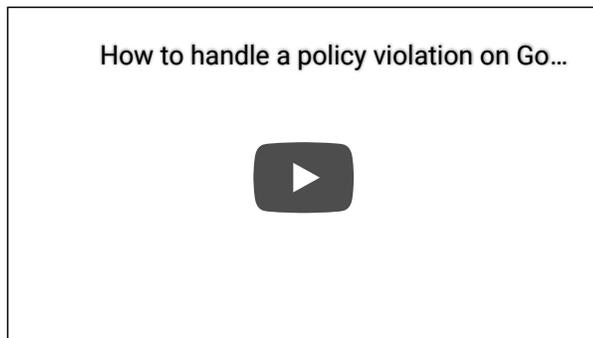
- Visibilitas aplikasi Anda dibatasi di Google Play. Aplikasi Anda akan tetap tersedia di Google Play dan dapat diakses oleh pengguna dengan link langsung ke listingan Play Store aplikasi.
- Status Visibilitas Terbatas yang ditetapkan pada aplikasi tidak akan memengaruhi status Akun Developer Google Play Anda.
- Status Visibilitas Terbatas yang ditetapkan pada aplikasi tidak akan memengaruhi kemampuan pengguna untuk melihat listingan Play Store, jumlah instal pengguna, statistik, dan rating yang sudah ada untuk aplikasi tersebut.

## Penghentian Akun

- Jika akun developer Anda dihentikan, semua aplikasi dalam katalog Anda akan dihapus dari Google Play dan Anda tidak dapat lagi memublikasikan aplikasi baru. Hal ini juga berarti bahwa setiap Akun Developer Google Play yang terkait akan ditangguhkan secara permanen.
- Penangguhan yang terjadi beberapa kali atau karena pelanggaran kebijakan yang berat juga dapat mengakibatkan penghentian akun Konsol Play Anda.
- Aplikasi dalam akun yang dihentikan akan dihapus, sehingga pengguna tidak akan dapat melihat listingan Play Store, jumlah instal pengguna yang sudah ada, statistik, dan rating untuk aplikasi tersebut.

Catatan: Setiap akun baru yang Anda buat akan turut dihentikan (tanpa pengembalian dana untuk biaya pendaftaran developer). Oleh karena itu, jangan coba mendaftar untuk mendapatkan akun Konsol Play baru jika salah satu akun Anda dihentikan.

## Mengelola dan Melaporkan Pelanggaran Kebijakan



## Mengajukan Banding terhadap Tindakan Penegakan

Kami akan mengaktifkan kembali aplikasi jika ternyata kami melakukan kekeliruan, dan kami mendapati bahwa aplikasi Anda tidak melanggar Kebijakan Program Google Play serta Perjanjian Distribusi Developer. Jika Anda telah meninjau kebijakan dengan cermat dan merasa bahwa keputusan kami keliru, ikuti petunjuk yang diberikan dalam pemberitahuan email penegakan untuk mengajukan banding atas keputusan kami.

## Referensi Tambahan

Jika memerlukan informasi lebih lanjut tentang tindakan penegakan atau rating/komentar dari pengguna, Anda dapat melihat beberapa referensi di bawah atau menghubungi kami melalui [Pusat Bantuan Google Play](#). Namun, kami tidak dapat memberikan nasihat hukum. Jika Anda memerlukan nasihat hukum, berkonsultasilah dengan penasihat hukum Anda.

- [Verifikasi & pengajuan banding aplikasi](#)
- [Melaporkan pelanggaran kebijakan](#)
- [Menghubungi Google Play perihal penghentian akun atau penghapusan aplikasi](#)
- [Peringatan wajar](#)
- [Melaporkan aplikasi & komentar yang tidak pantas](#)
- [Aplikasi saya telah dihapus dari Google Play](#)
- [Memahami penghentian Akun Developer Google Play](#)

---

Perlu bantuan lain?

Coba langkah-langkah selanjutnya berikut:

Hubungi kami

Beri tahu kami selengkapnya dan kami akan membantu Anda