Kebijakan Program Developer

(berlaku mulai 9 November 2022, kecuali jika dinyatakan lain)

Mari membangun sumber aplikasi dan game paling tepercaya di dunia

Inovasi Andalah 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 tepercaya 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 cocok untuk Google Play dan mematuhi undang-undang setempat.

Membahayakan Anak

Aplikasi yang tidak melarang pengguna untuk membuat, mengupload, atau mendistribusikan konten yang memfasilitasi eksploitasi atau pelecehan terhadap anak-anak akan langsung dihapus dari Google Play. Hal ini mencakup semua materi pelecehan seksual terhadap anak-anak. Untuk melaporkan konten di produk Google yang mungkin mengeksploitasi anak, klik **Laporkan penyalahgunaan** . Jika Anda menemukan konten semacam itu di tempat lain di internet, harap hubungi langsung penegak hukum di negara Anda .

Kami melarang penggunaan aplikasi yang membahayakan anak-anak. Hal ini termasuk, tetapi tidak terbatas pada, penggunaan aplikasi untuk mendorong perilaku predator terhadap anak-anak, seperti:

- Interaksi tidak pantas yang ditujukan kepada anak (misalnya, meraba atau membelai).
- Pembujuk-rayuan anak (misalnya, berteman dengan anak secara online untuk memfasilitasi kontak seksual dan/atau bertukar gambar seksual dengan anak itu baik secara online maupun offline).
- Seksualisasi anak di bawah umur (misalnya, gambar yang mendeskripsikan, mendorong, atau mendukung pelecehan seksual terhadap anak-anak atau penggambaran anak-anak dengan cara yang dapat mengakibatkan eksploitasi seksual terhadap anak-anak).
- Pemerasan seksual (misalnya, mengancam atau memeras anak dengan memanfaatkan akses sungguhan atau yang diklaim dimiliki ke gambar intim anak itu).
- Perdagangan anak (misalnya, mengiklankan atau membujuk anak untuk eksploitasi seksual komersial).

Kami akan mengambil tindakan yang sesuai, termasuk melaporkan ke National Center for Missing & Exploited Children, jika kami menemukan konten yang mengandung materi pelecehan seksual terhadap anak-anak. Jika Anda yakin ada anak yang berada dalam bahaya atau telah menjadi korban pelecehan, eksploitasi, atau perdagangan, harap hubungi penegak hukum setempat dan hubungi organisasi perlindungan anak yang tercantum di sini .

Selain itu, aplikasi yang menarik bagi anak-anak tetapi menyertakan tema dewasa tidak diizinkan termasuk, tetapi tidak terbatas pada:

- Aplikasi yang berisi kekerasan, darah, dan adegan menyeramkan yang berlebihan.
- Aplikasi yang menggambarkan atau memfasilitasi aktivitas 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.

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 Kata-Kata Tidak Sopan

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

Jika aplikasi berisi konten yang melanggar kebijakan ini tetapi konten tersebut dianggap pantas di wilayah tertentu, aplikasi tersebut mungkin tersedia bagi pengguna di wilayah tersebut, namun akan tetap tidak tersedia bagi pengguna di wilayah lain.

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.

- 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 kata-kata 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 tindakan seksual untuk mendapatkan imbalan, termasuk, tetapi tidak terbatas pada kencan berkompensasi atau pengaturan seksual ketika seorang peserta secara tersirat atau diharapkan memberikan uang, hadiah, atau dukungan keuangan kepada peserta lain (“sugar dating”).
- Aplikasi yang menurunkan harga diri atau menjadikan orang sebagai objek, seperti aplikasi yang mengklaim dapat menerawang pakaian, meskipun jika diberi label sebagai aplikasi trik tipuan atau hiburan.

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, kasta, status imigrasi, 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.

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 atau ucapan yang menyatakan bahwa suatu kelompok yang dilindungi tidak berperikemanusiaan, rendahan, atau patut 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 kegiatan berbahaya lainnya. Aplikasi yang menggambarkan kekerasan fiksi dalam konteks game, seperti kartun, berburu, atau memancing umumnya diperbolehkan.

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.

- Penggambaran grafis atau deskripsi kekerasan atau ancaman kekerasan yang realistis terhadap orang maupun hewan.
- Aplikasi yang mendorong tindakan bunuh diri, menyakiti diri sendiri, gangguan makan, mencekik leher (choking game), maupun tindakan lainnya yang dapat menyebabkan 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 konteks EDSA yang relevan.

Organisasi dan Gerakan Berbahaya

Kami tidak mengizinkan gerakan atau organisasi yang telah terlibat dalam, bersiap untuk, atau mengaku bertanggung jawab atas tindakan kekerasan terhadap warga sipil untuk memublikasikan aplikasi di Google Play untuk tujuan apa pun, termasuk perekrutan.

Kami tidak mengizinkan aplikasi dengan konten yang terkait dengan perencanaan, persiapan, atau pengagungan kekerasan terhadap warga sipil. Jika aplikasi Anda menyertakan konten tersebut untuk tujuan EDSA, konten tersebut harus diberikan beserta konteks EDSA yang relevan.

Peristiwa Sensitif

Kami tidak mengizinkan aplikasi yang memanfaatkan atau tidak sensitif terhadap peristiwa sensitif dengan dampak sosial, budaya, atau politik yang signifikan, seperti keadaan darurat sipil, bencana alam, keadaan kesehatan masyarakat, 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.

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.

- Kurangnya kepekaan mengenai kasus kematian seseorang atau sekelompok orang karena bunuh diri, overdosis, penyebab alami, dll.
- Tidak mengakui terjadinya peristiwa tragis besar yang terdokumentasi dengan baik.
- Tampak mencari keuntungan dari peristiwa sensitif tanpa manfaat nyata bagi korban.
- Aplikasi yang melanggar pedoman yang dijelaskan dalam artikel Persyaratan untuk aplikasi penyakit virus corona 2019 (COVID-19) .

Penindasan dan Pelecehan

Kami tidak mengizinkan aplikasi yang berisi atau memfasilitasi ancaman, pelecehan, atau penindasan.

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.

- Melakukan penindasan 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 cara mengonversi senjata api biasa menjadi senjata api otomatis, atau kemampuan menembak otomatis tersimulasi.

Ganja

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

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.

- 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.

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.

- 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 mengandung atau mempromosikan produk dan layanan keuangan, Anda harus mematuhi peraturan negara bagian dan lokal untuk wilayah atau negara mana pun yang menjadi target aplikasi Anda - misalnya, termasuk pengungkapan spesifik yang disyaratkan oleh undang-undang lokal.

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 pendidikan. 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
- Contoh tidak termasuk: Hipotek, kredit kendaraan bermotor, 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 memiliki Kategori Aplikasi yang ditetapkan ke "Keuangan" di Konsol Play dan 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 prinsip dan 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.

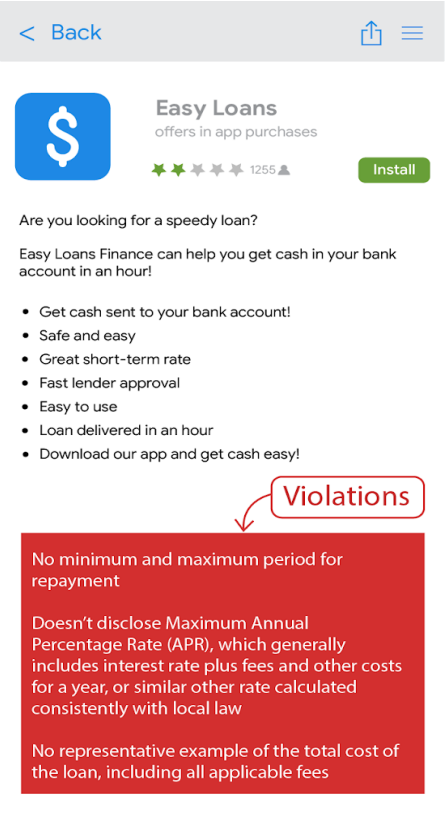
Persyaratan tambahan untuk aplikasi pinjaman pribadi di India, Indonesia, dan Filipina.

Aplikasi pinjaman pribadi di India, Indonesia, dan Filipina harus melengkapi bukti tambahan persyaratan kelayakan di bawah ini.

1. **India**
   - Lengkapi Pernyataan Aplikasi Pinjaman Pribadi untuk India dan berikan dokumentasi yang diperlukan untuk mendukung pernyataan Anda. Contoh:
     - Jika Anda diberi lisensi oleh Reserve Bank of India (RBI) untuk memberikan pinjaman pribadi, Anda harus menyerahkan salinan lisensi Anda untuk kami tinjau.
     - Jika Anda tidak terlibat secara langsung dalam aktivitas peminjaman uang dan hanya menyediakan platform untuk memfasilitasi peminjaman uang oleh Perusahaan Keuangan Non-Perbankan (NBFC) atau bank yang terdaftar kepada pengguna, Anda harus menyatakannya secara akurat dalam pernyataan.
       - Selain itu, nama semua NBFC dan bank yang terdaftar harus diungkapkan secara jelas dalam deskripsi aplikasi Anda.
   - Pastikan bahwa nama akun developer sesuai dengan nama bisnis terdaftar terkait yang diberikan melalui pernyataan Anda.
2. **Indonesia**
   - Lengkapi Pernyataan Aplikasi Pinjaman Pribadi untuk Indonesia , dan berikan dokumentasi yang diperlukan untuk mendukung pernyataan Anda. Contoh:
     - Jika aplikasi Anda terlibat dalam aktivitas Layanan Pinjam Meminjam Uang Berbasis Teknologi Informasi sesuai dengan Peraturan OJK No. 77/POJK.01/2016 (sebagaimana dapat diamandemen dari waktu ke waktu), Anda harus menyerahkan salinan lisensi Anda yang valid untuk kami tinjau.
   - Pastikan bahwa nama akun developer sesuai dengan nama bisnis terdaftar terkait yang diberikan melalui pernyataan Anda.
3. **Filipina**
   - Lengkapi Pernyataan Aplikasi Pinjaman Pribadi untuk Filipina , dan berikan dokumentasi yang diperlukan untuk mendukung pernyataan Anda.
     - Semua perusahaan keuangan dan peminjaman yang menawarkan pinjaman melalui Online Lending Platforms (OLP) harus memperoleh Nomor Pendaftaran SEC dan Nomor Certificate of Authority (CA) dari Philippines Securities and Exchanges Commission (PSEC).
       - Selain itu, Anda harus mengungkapkan Nama Perusahaan, Nama Bisnis, Nomor Pendaftaran PSEC, dan Certificate of Authority (CA) untuk Menjalankan Perusahaan Keuangan/Peminjaman dalam deskripsi aplikasi Anda.

- Aplikasi yang terlibat dalam aktivitas crowdfunding berbasis peminjaman, seperti peminjaman peer-to-peer (P2P), atau seperti yang ditetapkan dalam Aturan dan Regulasi yang Mengatur Crowdfunding (CF Rules), harus memproses transaksi melalui Perantara CF yang Terdaftar di PSEC.

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.



Perjudian

Kami mengizinkan aplikasi perjudian dengan uang, iklan yang terkait dengan perjudian dengan uang, program loyalitas dengan hasil berunsur game, dan aplikasi olahraga fantasi harian yang memenuhi persyaratan tertentu.

Aplikasi Perjudian

Sesuai dengan pembatasan dan kepatuhan terhadap semua kebijakan Google Play, kami mengizinkan aplikasi yang memungkinkan atau memfasilitasi perjudian online di negara tertentu asalkan Developer menyelesaikan proses pengajuan permohonan untuk aplikasi perjudian yang didistribusikan di Google Play, merupakan operator pemerintah yang disetujui dan/atau terdaftar sebagai operator berlisensi pada otoritas perjudian pemerintah yang sesuai di negara yang ditentukan, dan menyediakan lisensi operasional yang valid di negara yang ditentukan untuk jenis produk perjudian online yang ingin ditawarkan.

Kami hanya mengizinkan aplikasi perjudian berlisensi atau sah yang valid dengan jenis produk perjudian online berikut di dalamnya

- Game Kasino Online
- Taruhan Olahraga
- Pacuan Kuda (jika diatur dan diberi lisensi secara terpisah dari Taruhan Olahraga)
- Lotre

- Olahraga Fantasi Harian

Aplikasi yang valid 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 atau negara bagian/wilayah tempat aplikasi didistribusikan;
- Developer tidak boleh menawarkan jenis produk perjudian di luar cakupan lisensi perjudiannya;
- Aplikasi harus mencegah pengguna di bawah umur agar tidak menggunakan aplikasi;
- Aplikasi harus melarang akses dan penggunaan dari negara, negara bagian/wilayah, atau wilayah geografis yang tidak tercakup dalam 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 Google Play Store secara gratis;
- Aplikasi harus memiliki rating AO (Adult Only/Khusus Dewasa) atau setara dengan IARC; dan
- Aplikasi dan listingan aplikasinya harus secara jelas menampilkan informasi tentang perjudian yang bertanggung jawab.

Aplikasi Game, Kontes, dan Turnamen dengan Uang Lainnya

Untuk semua aplikasi lain yang tidak memenuhi persyaratan kelayakan aplikasi perjudian yang disebutkan di atas dan tidak disertakan dalam “Uji Coba Game dengan Uang Sungguhan Lainnya” yang disebutkan di bawah, 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, dan game yang menerima uang dan menawarkan hadiah uang tunai atau hal lain yang bernilai di dunia nyata (kecuali program yang diizinkan berdasarkan persyaratan Program Loyalitas yang Digamifikasi yang dijelaskan di bawah).

Contoh pelanggaran

- Game yang menerima uang dengan memberi kesempatan memenangkan hadiah fisik atau uang sebagai imbalannya
- Aplikasi yang memiliki elemen atau fitur navigasi (misalnya item menu, tab, tombol, WebView, dll.) yang menyertakan "pesan ajakan" untuk bertaruh, mempertaruhkan, atau berpartisipasi dalam game, kontes, atau turnamen menggunakan uang sungguhan, seperti aplikasi yang mengundang pengguna untuk memilih "BERTARUH" atau “DAFTAR” atau “IKUTI” turnamen agar berkesempatan memenangkan hadiah uang tunai.
- Aplikasi yang menerima atau mengelola taruhan, mata uang dalam aplikasi, kemenangan, atau setoran agar dapat berjudi, atau mendapatkan hadiah fisik atau uang.

Uji Coba Game dengan Uang Asli Lainnya

Kami terkadang akan melakukan uji coba dalam waktu terbatas untuk jenis game yang menggunakan uang asli di wilayah tertentu. Untuk mengetahui detailnya, lihat halaman Pusat Bantuan ini.

Program Loyalitas Berunsur Game

Jika diizinkan oleh hukum dan tidak tunduk pada persyaratan pemberian lisensi perjudian atau game lainnya, kami mengizinkan program loyalitas yang memberikan bonus kepada pengguna dengan hadiah atau uang sungguhan, yang tunduk pada persyaratan kelayakan Play Store berikut:

Untuk semua aplikasi (game dan non-game):

- Manfaat, keuntungan, atau reward program loyalitas harus secara jelas berupa tambahan dan berada di bawah semua transaksi uang yang memenuhi syarat dalam aplikasi (dengan transaksi uang memenuhi syarat yang harus berupa transaksi terpisah sebenarnya untuk menyediakan barang atau layanan yang berbeda dari program loyalitas) dan tidak boleh tunduk pada pembelian atau terikat dengan mode transaksi apa pun yang melanggar pembatasan kebijakan Game, Kontes, dan Perjudian dengan Uang.
  - Misalnya, tidak ada bagian dari transaksi uang yang memenuhi syarat yang dapat mewakili biaya atau taruhan untuk berpartisipasi dalam program loyalitas, dan transaksi uang yang memenuhi syarat tidak boleh mengakibatkan pembelian barang atau layanan di atas harga normal.

Untuk aplikasi Game :

- Reward atau poin loyalitas dengan manfaat, keuntungan, atau reward yang terkait dengan transaksi uang yang memenuhi syarat hanya dapat diberikan dan ditukarkan dengan basis rasio tetap. Rasio ini didokumentasikan secara jelas dalam aplikasi dan juga dalam aturan resmi yang tersedia secara publik untuk program. Selain itu, perolehan manfaat atau nilai yang dapat ditukarkan **tidak** boleh digunakan untuk bertaruh, diberikan, atau dilipatgandakan berdasarkan performa pengguna dalam game, atau berupa hasil berbasis peluang.

Untuk aplikasi non-Game:

- Reward atau poin loyalitas dapat diberikan untuk kontes atau sebagai hasil berbasis peluang jika memenuhi persyaratan yang disebutkan di bawah. Program loyalitas dengan manfaat, keuntungan, atau reward yang terkait dengan transaksi uang yang memenuhi syarat harus:
  - Memublikasikan aturan resmi untuk program dalam aplikasi.
  - Untuk program yang melibatkan sistem reward variabel, berbasis peluang, atau acak: harus mengungkapkan dalam persyaratan resmi untuk program tersebut 1) peluang untuk program reward apa pun yang menggunakan peluang tetap untuk menentukan reward dan 2) metode pemilihan (misalnya variabel yang digunakan untuk menentukan reward) untuk semua program serupa lainnya.
  - Menentukan jumlah pemenang tetap, batas waktu entri yang tetap, dan tanggal pemberian hadiah, per promosi, dalam persyaratan resmi program yang menawarkan undian atau promosi dengan konsep serupa lainnya.
  - Mendokumentasikan dengan jelas semua rasio tetap untuk akumulasi dan penukaran poin loyalitas atau reward loyalitas di aplikasi serta dalam persyaratan resmi program tersebut.

Jenis aplikasi dengan Program loyalitas	**Program loyalitas berunsur game dan reward yang bervariasi**	**Reward loyalitas berdasarkan rasio/jadwal tetap**	**Persyaratan dan Ketentuan program loyalitas diwajibkan**	**Persyaratan & Ketentuan harus mengungkapkan peluang atau metode pemilihan program loyalitas berbasis peluang apa pun**
Game	Tidak Diizinkan	Diizinkan	Wajib	T/A (Aplikasi game tidak diizinkan untuk menyertakan elemen berbasis peluang dalam program loyalitas)
Non-Game	Diizinkan	Diizinkan	Wajib	Wajib

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

Kami mengizinkan aplikasi dengan iklan yang mempromosikan perjudian, 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 ditampilkan;
- Iklan harus memenuhi semua persyaratan pemberian lisensi iklan setempat yang berlaku untuk semua produk dan layanan terkait perjudian yang dipromosikan;
- Aplikasi tidak boleh menampilkan iklan perjudian untuk individu yang berusia di bawah 18 tahun;
- Aplikasi tidak boleh didaftarkan di program Didesain untuk Keluarga;
- Aplikasi tidak boleh menargetkan individu berusia di bawah 18 tahun;
- Jika mengiklankan Aplikasi Perjudian (sebagaimana didefinisikan di atas), iklan harus secara jelas menampilkan informasi tentang perjudian yang bertanggung jawab di halaman landing aplikasi, di listingan aplikasi yang diiklankan itu sendiri, atau di dalam aplikasi;
- Aplikasi tidak boleh memberikan konten simulasi perjudian (misalnya aplikasi kasino sosial; aplikasi dengan mesin slot virtual);
- Aplikasi tidak boleh memberikan fungsi tambahan atau dukungan untuk perjudian atau game, lotre, atau turnamen dengan uang (misalnya fungsi yang membantu taruhan, pembayaran, pelacakan skor/peluang/performa peserta dalam pertandingan olahraga, atau pengelolaan dana partisipasi);
- Konten aplikasi tidak boleh mempromosikan atau mengarahkan pengguna ke layanan perjudian atau game, lotre, atau turnamen dengan uang

Hanya aplikasi yang memenuhi semua persyaratan di bagian yang tercantum (di atas) yang dapat menyertakan iklan untuk perjudian atau game, lotre, atau turnamen dengan uang. Aplikasi Perjudian yang disetujui (sebagaimana didefinisikan di atas), atau Aplikasi Olahraga Fantasi Harian yang disetujui (sebagaimana didefinisikan di bawah) yang memenuhi persyaratan 1-6 di atas, dapat menyertakan iklan untuk perjudian atau game, lotre, atau turnamen dengan uang.

Contoh pelanggaran

- Aplikasi yang didesain untuk pengguna di bawah umur dan menampilkan 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 yang menampilkan iklan perjudian yang melanggar kebijakan Iklan yang Menipu, seperti iklan yang ditampilkan kepada pengguna sebagai tombol, ikon, atau elemen interaktif lainnya di 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 dan proses pengajuan permohonan yang disebutkan di atas untuk negara selain Amerika Serikat;
- 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;

- Aplikasi dan listingan aplikasinya harus secara jelas menampilkan informasi tentang perjudian yang bertanggung jawab;
- Aplikasi harus mematuhi semua hukum dan standar industri yang berlaku untuk negara bagian Amerika Serikat atau wilayah Amerika Serikat mana pun tempat aplikasi tersebut didistribusikan;
- Developer harus memiliki lisensi yang valid untuk setiap negara bagian Amerika Serikat atau wilayah Amerika Serikat yang mewajibkan lisensi untuk aplikasi olahraga fantasi harian;
- Aplikasi harus melarang penggunaan dari Negara Bagian Amerika Serikat atau wilayah Amerika Serikat tempat developer tidak memiliki lisensi yang diperlukan untuk aplikasi olahraga fantasi harian; dan
- Aplikasi harus melarang penggunaan dari Negara Bagian Amerika Serikat atau wilayah Amerika Serikat yang tidak melegalkan aplikasi olahraga fantasi harian.

Aktivitas Ilegal

Kami tidak mengizinkan aplikasi yang memfasilitasi atau mempromosikan aktivitas ilegal.

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.

- Memfasilitasi penjualan atau pembelian obat-obatan terlarang.
- 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, termasuk aplikasi yang merupakan browser atau klien khusus untuk mengarahkan pengguna ke platform UGC, harus mengimplementasikan moderasi UGC yang ketat, efektif, dan berkelanjutan yang:

- 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 Google Play), dan melarangnya dalam persyaratan penggunaan atau kebijakan pengguna aplikasi;
- Melakukan moderasi UGC secara wajar dan sesuai dengan jenis UGC yang dihosting oleh aplikasi;
  - 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 untuk melaporkan pengguna dan UGC yang tidak pantas, serta mengambil tindakan terhadap UGC dan/atau pengguna tersebut jika perlu;
- Menyediakan sistem dalam aplikasi untuk memblokir UGC dan pengguna;
- Memberikan perlindungan untuk mencegah monetisasi dalam aplikasi agar tidak mendorong perilaku pengguna yang tidak menyenangkan.

Konten Seksual Insidental

Konten seksual dianggap “insidental” jika ditampilkan di aplikasi UGC yang (1) utamanya menyediakan akses ke konten non-seksual, dan (2) tidak secara aktif mempromosikan atau merekomendasikan konten seksual. Konten seksual ditetapkan sebagai konten ilegal oleh hukum yang berlaku dan konten membahayakan anak tidak dianggap “insidental” sehingga tidak diizinkan.

Aplikasi UGC dapat berisi konten seksual insidental jika semua persyaratan berikut dipenuhi:

- Konten tersebut disembunyikan secara default di balik filter yang memerlukan setidaknya dua tindakan pengguna untuk menonaktifkannya sepenuhnya (misalnya di balik interstisial obfuscation atau penayangannya dicegah secara default kecuali “penelusuran aman” dinonaktifkan).
- Anak-anak, seperti yang ditetapkan dalam Kebijakan keluarga, secara eksplisit dilarang mengakses aplikasi Anda melalui sistem verifikasi usia seperti layar verifikasi usia atau sistem yang sesuai seperti yang ditetapkan oleh hukum yang berlaku.
- Aplikasi Anda memberikan respons akurat terhadap kuesioner rating konten terkait UGC, sebagaimana yang diwajibkan oleh kebijakan Rating Konten .

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.

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.

- 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 penindasan, 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 gagal mengatasi keluhan pengguna tentang konten yang tidak pantas.

Layanan dan Konten Kesehatan

Kami tidak mengizinkan aplikasi yang menampilkan konten kesehatan dan layanan berbahaya kepada pengguna.

Jika aplikasi mengandung atau mempromosikan konten kesehatan dan layanan, Anda harus memastikan aplikasi mematuhi hukum dan peraturan yang berlaku.

Obat Resep

Kami tidak mengizinkan aplikasi yang memfasilitasi penjualan atau pembelian obat resep tanpa adanya resep.

Obat-obatan yang Tidak Disetujui

Google Play tidak mengizinkan aplikasi yang mempromosikan atau menjual obat-obatan yang tidak disetujui, terlepas dari klaim legalitas apa pun.

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.

- 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 yang dikendalikan.
- 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 yang dikendalikan 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 .

Misinformasi Kesehatan

Kami tidak mengizinkan aplikasi yang berisi klaim kesehatan menyesatkan dan bertentangan dengan konsensus medis yang ada, atau dapat membahayakan pengguna.

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.

- Klaim menyesatkan tentang vaksin, seperti vaksin yang dapat mengubah DNA seseorang.
- Advokasi untuk perawatan berbahaya dan tidak disetujui.
- Advokasi untuk praktik kesehatan berbahaya lain, seperti terapi konversi.

Batasan COVID-19

Aplikasi harus mengikuti artikel Persyaratan untuk aplikasi penyakit virus corona 2019 (COVID-19) .

Fungsi Medis

Kami tidak mengizinkan aplikasi yang menampilkan fungsi terkait medis atau kesehatan yang menyesatkan atau berpotensi berbahaya. Misalnya, kami tidak mengizinkan aplikasi yang mengklaim memiliki fungsi oksimetri yang hanya berbasis aplikasi. Aplikasi oksimeter harus didukung oleh hardware eksternal, perangkat wearable, atau sensor khusus yang disematkan di smartphone, yang dirancang untuk mendukung fungsi oksimetri. Aplikasi pendukung ini juga harus berisi pernyataan penyangkalan dalam metadata yang menyatakan bahwa aplikasi tidak ditujukan untuk penggunaan medis, hanya dirancang untuk tujuan kebugaran dan kesehatan umum, bukan perangkat medis, dan harus mengungkapkan dengan benar model hardware/model perangkat yang kompatibel.

Pembayaran - Layanan Klinis

Transaksi yang melibatkan layanan klinis yang diatur tidak boleh menggunakan sistem penagihan Google Play. Untuk informasi selengkapnya, lihat Memahami kebijakan Pembayaran Google Play .

Data Health Connect

Data yang diakses melalui Izin Health Connect dianggap sebagai data pengguna yang bersifat pribadi dan sensitif yang tunduk pada kebijakan Data Pengguna , dan tunduk pada persyaratan tambahan .

Kekayaan Intelektual

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

Kami akan menanggapi 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, silakan kirim pemberitahuan pemalsuan .

Jika Anda adalah pemilik merek dagang dan yakin bahwa ada aplikasi di Google Play yang melanggar hak merek dagang Anda, silakan hubungi developer secara langsung untuk menyampaikan kekhawatiran Anda. Jika tidak dapat menemukan penyelesaian masalah dengan developer, kirimkan keluhan merek dagang 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 merek, logo, dan aset visual), hubungi tim Google Play sebelum mengirimkannya untuk memastikan aplikasi Anda 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 fungsionalitas aplikasi Anda. Secara umum, pendekatan yang paling aman adalah dengan membuat konten asli.

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.

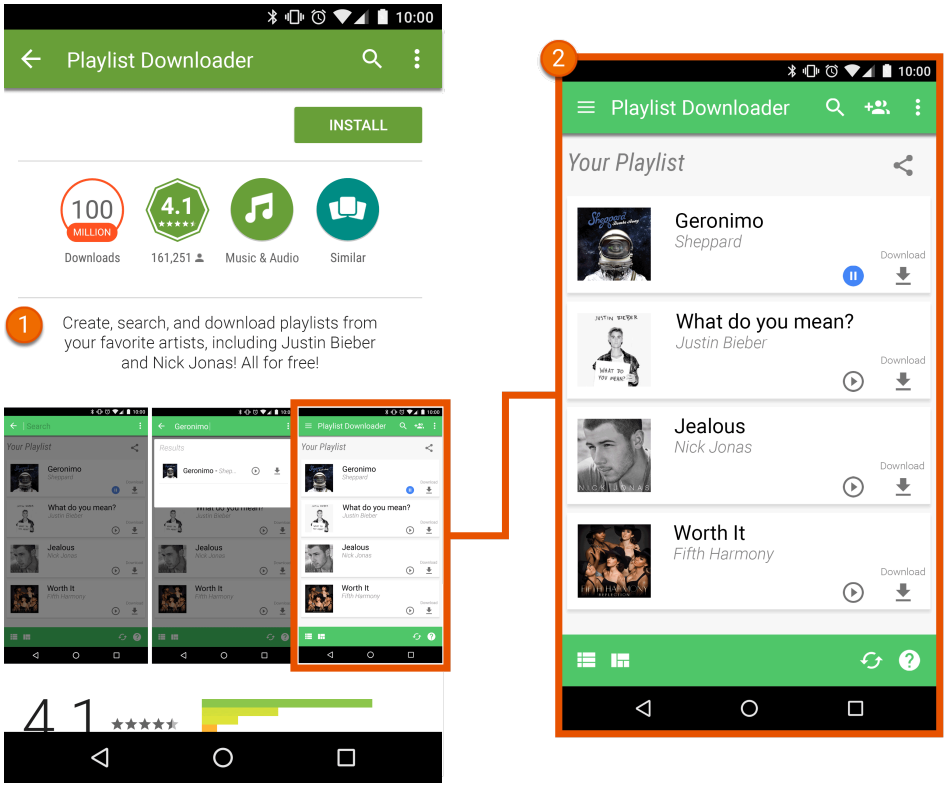
- Gambar seni sampul untuk album musik, game video, dan buku.
- Gambar pemasaran dari film, televisi, atau video game.
- Karya seni atau gambar dari buku komik, kartun, film, video musik, atau televisi.
- Logo tim olahraga profesional atau sekolah.
- Foto yang diambil dari akun media sosial tokoh terkenal.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

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.

- Aplikasi streaming yang memungkinkan pengguna mendownload salinan lokal konten berhak cipta tanpa izin.
- Aplikasi yang mendorong pengguna untuk menstreaming dan mendownload karya berhak cipta, termasuk musik dan video, 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.

Palsu

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 ini meniru fitur merek produk agar dapat disamarkan 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 secara transparan menunjukkan 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 dan sensitif, harap lihat persyaratan tambahan pada bagian "Data Pengguna yang Bersifat 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. Jika Anda menyertakan kode pihak ketiga (misalnya SDK) di aplikasi Anda, Anda harus memastikan bahwa kode pihak ketiga yang digunakan di aplikasi Anda mematuhi kebijakan Program Developer Google Play.

Data Pengguna yang Bersifat Pribadi dan Sensitif

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

- Membatasi pengaksesan, pengumpulan, penggunaan, dan pembagian oleh Anda atas data pengguna yang bersifat pribadi dan sensitif yang diperoleh melalui aplikasi untuk tujuan yang terkait secara langsung dengan penyediaan dan peningkatan kualitas fitur aplikasi (misalnya, fungsi yang diharapkan pengguna yang didokumentasikan dan dipromosikan dalam deskripsi aplikasi di Google Play). Berbagi data pengguna yang bersifat pribadi dan sensitif termasuk menggunakan SDK atau layanan pihak ketiga lainnya yang menyebabkan data ditransfer ke pihak ketiga. Aplikasi yang memperluas penggunaan data pengguna yang bersifat pribadi dan sensitif untuk menayangkan iklan harus mematuhi Kebijakan Iklan kami.
- Menangani semua data pengguna yang bersifat pribadi dan sensitif dengan aman, termasuk mengirimkannya melalui kriptografi modern (misalnya, melalui HTTPS).
- Selalu menggunakan permintaan izin runtime jika tersedia, sebelum mengakses data yang dilindungi oleh izin Android .
- Tidak menjual data pengguna yang bersifat pribadi dan sensitif.

Persyaratan Pengungkapan & Izin yang Jelas

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

Anda harus menyediakan pengungkapan dalam aplikasi terkait pengaksesan, pengumpulan, penggunaan, dan pembagian 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 pengguna yang bersifat pribadi dan sensitif.

Pengungkapan dalam aplikasi Anda harus disertakan dengan dan langsung mendahului permintaan izin pengguna dan, jika memungkinkan, izin runtime yang terkait. Anda tidak boleh mengakses atau mengumpulkan data yang bersifat pribadi dan sensitif apa pun hingga pengguna mengizinkan. Permintaan izin aplikasi:

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

Untuk memenuhi persyaratan kebijakan, sebaiknya Anda merujuk pada contoh format untuk Pengungkapan yang Jelas berikut saat diperlukan:

- "[Aplikasi ini] mengumpulkan/mentransmisikan/menyinkronkan/menyimpan [jenis data] untuk mengaktifkan ["fitur"], [dalam skenario seperti apa]."
- *Contoh: "Fitness Funds mengumpulkan data lokasi untuk mengaktifkan pelacakan kebugaran bahkan saat aplikasi ditutup atau tidak digunakan. Data tersebut juga digunakan untuk mendukung iklan".*
- *Contoh: "Call buddy mengumpulkan data log panggilan baca dan tulis untuk mengaktifkan pengaturan kontak bahkan saat aplikasi tidak digunakan".*

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.

- Aplikasi yang mengumpulkan lokasi perangkat tetapi tidak memiliki pengungkapan yang jelas terkait fitur mana yang menggunakan data ini dan/atau menunjukkan penggunaan aplikasi di latar belakang.
- Aplikasi yang memiliki izin runtime dan meminta akses ke data **sebelum** pengungkapan yang jelas untuk menetapkan tujuan penggunaan data.
- 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 untuk Akses Data yang Bersifat Pribadi dan 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 Anda tidak boleh mengungkapkan data pengguna apa pun yang bersifat sensitif dan 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	Aplikasi Anda harus memposting kebijakan privasi, beserta pengungkapan dalam aplikasi, yang menjelaskan data pengguna yang dikumpulkan dan

antivirus, anti-malware, atau fitur terkait keamanan	ditransmisikan oleh aplikasi Anda, penggunaannya, dan dengan siapa data tersebut akan dibagikan.
Aplikasi Anda menargetkan anak-anak	Aplikasi Anda tidak boleh menyertakan SDK yang tidak disetujui penggunaannya dalam layanan yang ditujukan untuk anak-anak. Lihat Mendesain Aplikasi untuk Anak-Anak dan Keluarga untuk mengetahui persyaratan dan bahasa kebijakan lengkap.
Aplikasi Anda mengumpulkan atau menautkan ID perangkat tetap (misalnya IMEI, IMSI, Seri SIM #, dll.)	ID perangkat tetap tidak boleh ditautkan ke data pengguna lainnya yang bersifat pribadi dan sensitif atau ID perangkat yang dapat direset kecuali untuk tujuan • Telepon yang ditautkan ke identitas kartu SIM (misalnya, panggilan Wi-Fi yang ditautkan ke akun operator), dan • Aplikasi pengelolaan perangkat perusahaan menggunakan mode pemilik perangkat. Penggunaan ini harus diungkapkan secara jelas kepada pengguna sebagaimana ditentukan dalam Kebijakan Data Pengguna . Harap baca referensi ini untuk mengetahui ID unik alternatif. Harap baca Kebijakan iklan untuk mendapatkan panduan tambahan untuk ID Iklan Android.

Bagian keamanan data

Semua developer harus melengkapi bagian Keamanan data yang jelas dan akurat untuk setiap aplikasi yang memberikan detail terkait pengumpulan, penggunaan, dan pembagian data pengguna. Developer bertanggung jawab atas akurasi label dan menjaga agar informasi ini tetap diperbarui. Jika relevan, bagian tersebut harus konsisten dengan pengungkapan yang dibuat dalam kebijakan privasi aplikasi.

Harap lihat artikel ini untuk mengetahui informasi tambahan tentang cara melengkapi bagian Keamanan data.

Kebijakan Privasi

Semua aplikasi harus memposting link kebijakan privasi di kolom yang ditetapkan di Konsol Play, dan link atau teks kebijakan privasi di 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, yang tidak dibatasi oleh data yang diungkapkan dalam label privasi. Informasi ini harus mencakup:

- Informasi developer dan kontak privasi atau mekanisme untuk mengajukan pertanyaan.
- Mengungkapkan jenis data pengguna yang bersifat pribadi dan sensitif yang diakses, dikumpulkan, digunakan, dan dibagikan aplikasi Anda; dan pihak mana pun yang Anda ajak bekerja sama untuk berbagi data pengguna yang bersifat pribadi atau sensitif
- Prosedur penanganan data yang aman untuk data pengguna yang bersifat pribadi dan sensitif.
- Kebijakan retensi dan penghapusan data developer.
- Pelabelan kebijakan privasi yang jelas (misalnya, tercantum sebagai “kebijakan privasi” dalam judul).

Entitas (misalnya, developer atau perusahaan) yang disebutkan dalam listingan Google Play Store aplikasi harus muncul dalam kebijakan privasi atau aplikasi harus diberi nama dalam kebijakan privasi. Aplikasi yang tidak mengakses data pengguna yang bersifat pribadi dan sensitif tetap harus mengirimkan kebijakan privasi.

Pastikan kebijakan privasi Anda tersedia dalam URL (bukan PDF) aktif yang dapat di akses secara publik dan tidak dibatasi oleh wilayah dan tidak dapat diedit.

Penggunaan ID Kumpulan Aplikasi

Android akan memperkenalkan ID baru untuk mendukung kasus penggunaan penting seperti analisis dan pencegahan penipuan. Persyaratan untuk penggunaan ID ini dijelaskan di bawah.

- **Penggunaan**: ID kumpulan aplikasi tidak boleh digunakan untuk personalisasi iklan dan pengukuran iklan.
- **Keterkaitan dengan informasi identitas pribadi atau ID lainnya:** ID kumpulan aplikasi tidak boleh terhubung ke ID Android apa pun (misalnya AAID) atau data pribadi dan sensitif apa pun untuk tujuan iklan.
- **Transparansi dan izin:** Pengumpulan dan penggunaan ID kumpulan aplikasi dan komitmen terhadap persyaratan ini harus diungkapkan kepada pengguna dalam pemberitahuan privasi yang memadai secara hukum, termasuk kebijakan privasi Anda. Anda harus mendapatkan izin yang sah secara hukum dari pengguna jika diperlukan. Untuk mempelajari standar privasi kami lebih lanjut, harap tinjau kebijakan Data Pengguna kami.

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

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 undang-undang privasi, keamanan data, dan perlindungan data, serta instruksi, regulasi, dan peraturan yang berlaku;
- Mengakses, menggunakan, atau memproses Informasi Pribadi Uni Eropa (EU) hanya untuk tujuan yang sesuai dengan izin yang didapatkan dari pengguna yang berkaitan dengan Informasi Pribadi Uni Eropa tersebut;
- Menerapkan langkah-langkah teknis dan organisasi yang sesuai untuk melindungi Informasi Pribadi UE dari kehilangan, penyalahgunaan, serta akses, pengungkapan, pengubahan, dan perusakan yang tidak sah atau melanggar hukum; dan
- Memberikan tingkat perlindungan yang sama seperti yang diwajibkan oleh Privacy Shield Principles .

Anda harus memantau kepatuhan Anda dengan 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 dan segera menghentikan pemrosesan Informasi Pribadi Uni Eropa, atau melakukan langkah-langkah yang wajar dan sesuai untuk memulihkan perlindungan ke tingkat yang memadai.

Per tanggal 16 Juli 2020, Google tidak lagi mengandalkan EU-U.S. Privacy Shield (Perlindungan Privasi EU-AS) untuk mentransfer data pribadi yang berasal dari Wilayah Ekonomi Eropa atau Inggris Raya ke Amerika Serikat. (Pelajari Lebih Lanjut.)Informasi selengkapnya ditetapkan dalam DDA Pasal 9.

Izin dan API yang Mengakses Informasi Sensitif

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

Mintalah izin dan API yang mengakses informasi sensitif untuk mengakses data sesuai konteks (melalui permintaan 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 tersebut menyetujui penggunaan tambahan tersebut.

Izin Terbatas

Selain hal di atas, izin terbatas adalah izin yang ditetapkan sebagai Berbahaya , Khusus , Tanda Tangan , atau seperti yang didokumentasikan di bawah. Izin ini 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 memperbaiki fitur atau layanan saat ini dalam aplikasi yang datanya dikumpulkan. Anda juga boleh mentransfer data sebagaimana yang diperlukan untuk mematuhi hukum 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 akses ke Log Panggilan dibatasi).
- Penggunaan izin yang bertentangan dengan Praktik terbaik Izin aplikasi developer Android resmi atau melanggar kebijakan yang ada (termasuk Penyalahgunaan Hak Istimewa yang Ditingkatkan), secara tegas dilarang.

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 pribadi dan sensitif yang tunduk pada kebijakan Informasi Pribadi dan Sensitif , dan batasan berikut:

Izin Terbatas	Persyaratan
Grup izin Log Panggilan (misanya, READ_CALL_LOG, WRITE_CALL_LOG, PROCESS_OUTGOING_CALLS)	Izin harus terdaftar secara aktif sebagai pengendali Telepon atau Asisten default di perangkat.
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 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 secara jelas didokumentasikan dan dijelaskan dalam deskripsi aplikasi. Tanpa fitur inti, aplikasi 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 dikaitkan 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 dan kebijakan Lokasi Latar Belakang, dan 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 menayangkan 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 memiliki ekspektasi yang wajar bahwa fitur atau layanan tersebut memerlukan tingkat 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 penggunaannya:

- 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 .

Untuk mengetahui informasi selengkapnya terkait persyaratan kebijakan, harap buka artikel bantuan ini .

Izin Akses Semua File

Atribut direktori dan file 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 penting aplikasi yang berhubungan dengan pengguna.
- Perangkat Android yang menjalankan versi R 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 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 persyaratan versi R lebih lanjut, harap buka artikel bantuan ini.

Izin Visibilitas Paket (Aplikasi)

Inventaris aplikasi terinstal yang dikueri dari perangkat dianggap sebagai data pengguna yang bersifat pribadi dan sensitif, yang tunduk pada kebijakan Informasi Pribadi dan Sensitif , serta persyaratan berikut:

Aplikasi yang memiliki tujuan inti untuk meluncurkan, menelusuri, atau berinteroperasi dengan aplikasi lain di perangkat, dapat memperoleh visibilitas yang sesuai cakupan pada aplikasi terinstal lainnya di perangkat, seperti yang diuraikan di bawah ini:

- **Visibilitas aplikasi yang luas:** Visibilitas luas adalah kemampuan aplikasi untuk memperoleh visibilitas yang ekstensif (atau "luas") pada aplikasi terinstal ("paket") di perangkat.
  - Untuk aplikasi yang menarget API level 30 atau yang lebih baru , visibilitas luas pada aplikasi terinstal melalui izin QUERY_ALL_PACKAGES dibatasi untuk kasus penggunaan tertentu ketika kesadaran dan/atau interoperabilitas dengan salah satu dan semua aplikasi di perangkat diperlukan agar aplikasi dapat berfungsi.
    - Anda tidak boleh menggunakan QUERY_ALL_PACKAGES jika aplikasi Anda dapat beroperasi dengan deklarasi visibilitas paket tercakup yang lebih ditargetkan (mis. mengajukan kueri dan berinteraksi dengan paket tertentu, bukannya meminta visibilitas luas).
  - Penggunaan metode alternatif yang menyerupai tingkat visibilitas luas yang terkait dengan izin QUERY_ALL_PACKAGES juga dibatasi untuk fungsi aplikasi inti yang dapat dilihat pengguna dan interoperabilitas dengan aplikasi apa pun yang ditemukan melalui metode ini.
  - Harap lihat artikel Pusat Bantuan ini untuk mengetahui kasus penggunaan yang diizinkan terkait izin QUERY_ALL_PACKAGES.
- **Visibilitas aplikasi yang terbatas**: Visibilitas terbatas adalah saat aplikasi meminimalkan akses ke data dengan mengajukan kueri untuk aplikasi tertentu menggunakan metode yang lebih ditargetkan (bukan metode “luas”) (mis. mengajukan kueri untuk aplikasi tertentu yang memenuhi deklarasi manifes aplikasi Anda). Anda dapat menggunakan metode ini guna mengajukan kueri untuk aplikasi Anda yang memiliki interoperabilitas yang sesuai dengan kebijakan, atau untuk pengelolaan aplikasi tersebut.
- Visibilitas ke inventaris aplikasi terinstal di perangkat harus berkaitan langsung dengan tujuan inti atau fungsi inti yang diakses pengguna dalam aplikasi Anda.

Data inventaris aplikasi yang dikueri dari aplikasi yang didistribusikan oleh Google Play tidak boleh dijual atau dibagikan untuk tujuan monetisasi iklan atau analisis.

Accessibility API

Accessibility API tidak dapat digunakan untuk:

- Mengubah setelan pengguna tanpa izin mereka atau mencegah kemampuan pengguna untuk menonaktifkan atau meng-uninstal aplikasi atau layanan apa pun kecuali jika diizinkan oleh orang tua atau wali melalui aplikasi kontrol orang tua atau oleh administrator resmi melalui software pengelolaan perusahaan;
- Mengakali kontrol privasi dan notifikasi bawaan Android; atau
- Mengubah atau memanfaatkan antarmuka pengguna dengan cara yang menipu atau melanggar Kebijakan Developer Google Play.

Accessibility API tidak dirancang dan tidak diminta untuk perekaman audio jarak jauh.

Penggunaan Accessibility API harus didokumentasikan dalam listingan Google Play.

Panduan untuk IsAccessibilityTool

Aplikasi dengan fungsi inti yang dimaksudkan untuk secara langsung mendukung difabel memenuhi syarat untuk menggunakan **IsAccessibilityTool** agar dapat ditetapkan sebagai aplikasi aksesibilitas secara publik dan dengan tepat.

Aplikasi yang tidak memenuhi syarat untuk **IsAccessibilityTool** tidak boleh menggunakan tanda tersebut dan harus memenuhi persyaratan pengungkapan dan izin yang jelas seperti yang diuraikan dalam kebijakan Data Pengguna karena fungsi terkait aksesibilitas tidak jelas bagi pengguna. Harap lihat artikel pusat bantuan AccessibilityService API untuk mendapatkan informasi selengkapnya.

Aplikasi harus menggunakan API dan izin yang terbatas cakupannya sebagai pengganti Accessibility API jika memungkinkan, untuk mencapai fungsi yang diinginkan.

Izin Minta Instal Paket

Izin REQUEST_INSTALL_PACKAGES memungkinkan aplikasi meminta penginstalan paket aplikasi. Untuk menggunakan izin ini, fungsi inti aplikasi Anda harus mencakup:

- Mengirim atau menerima paket aplikasi; dan
- Memungkinkan penginstalan paket aplikasi yang dimulai oleh pengguna.

Fungsi yang diizinkan mencakup:

- Penelusuran atau penjelajahan web; atau
- Layanan komunikasi yang memiliki fitur lampiran; atau
- Pengelolaan, transfer, atau berbagi file; atau
- Pengelolaan perangkat perusahaan.
- Pencadangan & pemulihan
- Migrasi Perangkat/Pemindahan Data Ponsel

Fungsi inti didefinisikan sebagai tujuan utama aplikasi. Fungsi inti, serta fitur inti apa pun yang membentuk fungsi inti ini, harus didokumentasikan dan dipromosikan dengan jelas dalam deskripsi aplikasi.

Izin REQUEST_INSTALL_PACKAGES tidak dapat digunakan untuk menjalankan update mandiri, modifikasi, atau pemaketan APK lain dalam file aset kecuali untuk tujuan pengelolaan perangkat. Semua proses update atau penginstalan paket harus mematuhi kebijakan Penyalahgunaan Jaringan dan Perangkat Google Play dan harus dimulai dan didorong oleh pengguna.

Health Connect dengan Izin Android

Data yang diakses melalui Izin Health Connect dianggap sebagai data pengguna yang bersifat pribadi dan sensitif yang tunduk pada kebijakan Data Pengguna, serta persyaratan tambahan berikut:

Akses dan Penggunaan Health Connect yang tepat

Permintaan untuk mengakses data melalui Health Connect harus jelas dan dapat dipahami. Health Connect hanya dapat digunakan sesuai dengan persyaratan dan ketentuan, serta kebijakan yang berlaku, dan untuk kasus penggunaan yang disetujui sebagaimana ditetapkan dalam kebijakan ini. Artinya, Anda hanya dapat meminta akses ke izin jika aplikasi atau layanan Anda memenuhi salah satu kasus penggunaan yang disetujui.

Berikut kasus penggunaan yang disetujui untuk mengakses Izin Health Connect:

- Aplikasi atau layanan dengan satu atau beberapa fitur yang bermanfaat bagi kesehatan dan kebugaran pengguna. Fitur tersebut harus tersedia melalui antarmuka pengguna yang memungkinkan mereka secara langsung **mencatat, melaporkan, memantau, dan/atau menganalisis** aktivitas fisik, tidur, kesehatan mental, nutrisi, indikator kesehatan, kondisi tubuh, dan/atau indikator serta kondisi lain terkait kesehatan atau kebugaran.
- Aplikasi atau layanan dengan satu atau beberapa fitur yang bermanfaat bagi kesehatan dan kebugaran pengguna. Fitur tersebut harus tersedia melalui antarmuka pengguna yang memungkinkan pengguna **menyimpan** data terkait aktivitas fisik, tidur, kesehatan mental, nutrisi, indikator kesehatan, kondisi tubuh, dan/atau indikator serta kondisi lain terkait kesehatan atau kebugaran di ponsel dan/atau perangkat wearable mereka, serta membagikan data mereka ke aplikasi lain di perangkat yang memenuhi kasus penggunaan ini.

Health Connect adalah platform penyimpanan dan berbagi data untuk tujuan umum yang memungkinkan pengguna menggabungkan data kesehatan dan kebugaran dari berbagai sumber di perangkat Android mereka. Pengguna juga dapat membagikannya kepada pihak ketiga pilihan mereka. Data tersebut dapat berasal dari berbagai sumber sebagaimana ditentukan oleh pengguna. Developer

harus menilai apakah Health Connect sesuai dengan tujuan penggunaan mereka. Developer juga harus menyelidiki serta memeriksa sumber dan kualitas semua data dari Health Connect sehubungan dengan tujuan apa pun, khususnya untuk penggunaan medis, kesehatan, atau riset.

- Aplikasi yang melakukan riset kesehatan pada manusia dengan data yang diperoleh melalui Health Connect harus mendapatkan izin dari peserta atau, untuk anak di bawah umur, dari orang tua atau wali mereka. Izin tersebut harus mencakup (a) sifat, tujuan, dan durasi penelitian; (b) prosedur, risiko, dan manfaat bagi peserta; (c) informasi tentang kerahasiaan dan penanganan data (termasuk pembagian apa pun dengan pihak ketiga); (d) kontak (POC) untuk menjawab pertanyaan peserta; dan (e) proses pembatalan partisipasi. Aplikasi yang melakukan riset kesehatan pada manusia dengan data yang diperoleh melalui Health Connect harus mendapatkan persetujuan dari dewan independen yang 1) bertujuan melindungi hak, keselamatan, serta kesejahteraan peserta dan 2) memiliki wewenang untuk meninjau, mengubah, serta menyetujui riset yang melibatkan manusia. Bukti persetujuan tersebut harus diberikan sesuai permintaan.
- Anda juga bertanggung jawab untuk memastikan kepatuhan terhadap persyaratan hukum atau peraturan yang mungkin berlaku berdasarkan tujuan penggunaan Health Connect dan data apa pun dari platform tersebut. Kecuali dinyatakan secara eksplisit dalam label atau informasi yang diberikan Google untuk produk atau layanan tertentu, Google tidak menjamin keakuratan data yang terdapat di Health Connect serta tidak mendukung penggunaan data tersebut untuk tujuan apa pun, khususnya penggunaan medis, kesehatan, atau riset. Google menyangkal semua kewajiban yang berhubungan dengan penggunaan data yang diperoleh melalui Health Connect.

Penggunaan Terbatas

Saat menggunakan Health Connect untuk penggunaan yang tepat, penggunaan Anda atas data yang diakses melalui Health Connect juga harus mematuhi persyaratan di bawah. Persyaratan ini berlaku untuk data mentah yang diperoleh dari Health Connect, serta data yang digabungkan, telah dilakukan de-identifikasi, atau berasal dari data mentah.

- Batasi penggunaan data Health Connect untuk menyediakan atau meningkatkan kualitas fitur atau kasus penggunaan yang tepat, yang terlihat dan tampak jelas di antarmuka pengguna aplikasi yang meminta.
- Hanya transfer data pengguna kepada pihak ketiga:
  - Untuk menyediakan atau meningkatkan kualitas fitur atau kasus penggunaan yang tepat yang tampak jelas dari antarmuka pengguna aplikasi yang meminta, dan hanya dengan izin pengguna;
  - Jika diperlukan untuk tujuan keamanan (misalnya, menyelidiki penyalahgunaan);
  - Untuk mematuhi hukum dan/atau peraturan yang berlaku; atau,
  - Sebagai bagian dari merger, akuisisi, atau penjualan aset developer setelah mendapatkan izin eksplisit sebelumnya dari pengguna.
- Jangan izinkan orang membaca data pengguna, kecuali:
  - Telah mendapatkan izin eksplisit dari pengguna untuk membaca data tertentu;
  - Izin tersebut diperlukan untuk tujuan keamanan (misalnya, menyelidiki penyalahgunaan);
  - Untuk mematuhi hukum yang berlaku; atau,
  - Data (termasuk turunannya) digabungkan dan digunakan untuk operasi internal sesuai dengan privasi yang berlaku serta persyaratan hukum yurisdiksi lainnya.

Semua transfer, penggunaan, atau penjualan data Health Connect lainnya dilarang, termasuk:

- Mentransfer atau menjual data pengguna kepada pihak ketiga seperti platform periklanan, broker data, atau distributor informasi apa pun.
- Mentransfer, menjual, atau menggunakan data pengguna untuk menayangkan iklan, termasuk iklan yang dipersonalisasi atau menurut minat.
- Mentransfer, menjual, atau menggunakan data pengguna untuk menentukan kelayakan kredit atau untuk tujuan pinjaman.

- Mentransfer, menjual, atau menggunakan data pengguna dengan produk atau layanan apa pun yang mungkin memenuhi syarat sebagai perangkat medis berdasarkan Pasal 201(h) Federal Food Drug & Cosmetic Act, jika data pengguna tersebut akan digunakan oleh perangkat medis untuk menjalankan fungsinya yang diatur oleh hukum.
- Mentransfer, menjual, atau menggunakan data pengguna untuk tujuan apa pun atau dengan cara yang melibatkan Informasi Kesehatan Terlindungi (sebagaimana dijelaskan dalam HIPAA), kecuali jika Anda mendapatkan persetujuan tertulis sebelumnya dari Google untuk penggunaan tersebut.

Akses ke Health Connect tidak boleh digunakan dengan cara yang melanggar kebijakan ini, atau persyaratan dan ketentuan atau kebijakan Health Connect lainnya yang berlaku, termasuk untuk tujuan berikut:

- Jangan menggunakan Health Connect untuk mengembangkan, atau untuk digabungkan ke dalam, aplikasi, lingkungan, atau aktivitas yang penggunaan atau kegagalannya secara wajar dapat diperkirakan menyebabkan kematian, cedera diri, atau kerusakan lingkungan/properti (seperti pembuatan atau pengoperasian fasilitas nuklir, kontrol lalu lintas udara, sistem bantuan hidup, atau persenjataan).
- Jangan mengakses data yang diperoleh melalui Health Connect dengan aplikasi headless. Aplikasi harus menampilkan ikon yang dapat diidentifikasi dengan jelas di baki aplikasi, setelan aplikasi perangkat, ikon notifikasi, dll.
- Jangan menggunakan Health Connect dengan aplikasi yang menyinkronkan data antara perangkat atau platform yang tidak kompatibel.
- Health Connect tidak dapat terhubung ke aplikasi, layanan, atau fitur yang hanya menargetkan anak-anak. Health Connect tidak disetujui untuk digunakan dalam layanan yang terutama ditujukan untuk anak-anak.

Anda harus mengungkapkan pernyataan afirmatif di aplikasi atau di situs milik layanan web atau aplikasi Anda bahwa penggunaan Anda atas data Health Connect mematuhi batasan Penggunaan Terbatas. Misalnya, menyediakan link di halaman beranda ke kebijakan privasi atau halaman khusus yang menyatakan: "Penggunaan informasi yang diterima dari Health Connect akan mematuhi kebijakan Izin Health Connect, termasuk persyaratan Penggunaan Terbatas."

Cakupan Minimum

Anda hanya dapat meminta akses ke izin yang penting untuk penerapan fungsi aplikasi atau layanan Anda.

Artinya:

- Jangan meminta akses ke informasi yang tidak diperlukan. Hanya minta akses ke izin yang diperlukan untuk menerapkan fitur atau layanan produk Anda. Jika produk Anda tidak memerlukan akses ke izin tertentu, Anda tidak boleh meminta akses ke izin ini.

Pemberitahuan dan Kontrol yang Transparan dan Akurat

Health Connect menangani data kesehatan dan kebugaran, yang mencakup informasi pribadi dan sensitif. Semua aplikasi dan layanan harus menyertakan kebijakan privasi. Kebijakan ini harus secara komprehensif mengungkapkan cara aplikasi atau layanan Anda mengumpulkan, menggunakan, dan membagikan data pengguna. Pengungkapan ini mencakup pihak seperti apa yang Anda ajak bekerja sama untuk berbagi data pengguna, cara Anda menggunakan data, cara Anda menyimpan dan mengamankan data, serta hal yang terjadi dengan data saat akun dinonaktifkan dan/atau dihapus.

Selain persyaratan berdasarkan hukum yang berlaku, Anda juga harus mematuhi persyaratan berikut:

- Anda harus menyediakan pengungkapan terkait pengaksesan, pengumpulan, penggunaan, dan pembagian data oleh Anda. Pengungkapan:
  - Harus secara akurat menunjukkan identitas aplikasi atau layanan yang berupaya mengakses data pengguna;

- Harus memberikan informasi yang jelas dan akurat yang menjelaskan jenis data yang diakses, diminta, dan/atau dikumpulkan;
- Harus menjelaskan cara data akan digunakan dan/atau dibagikan: Jika Anda meminta data untuk suatu alasan, tetapi juga akan menggunakan data tersebut untuk tujuan lainnya, Anda harus memberi tahu pengguna tentang kedua kasus penggunaan tersebut.

- Anda harus memberikan dokumentasi bantuan kepada pengguna yang menjelaskan tentang cara mengelola dan menghapus data mereka dari aplikasi Anda.

Penanganan Data yang Aman

Anda harus menangani semua data pengguna dengan aman. Ambil langkah yang wajar dan tepat untuk melindungi semua aplikasi atau sistem yang menggunakan Health Connect dari pengungkapan, perubahan, kehilangan, perusakan, penggunaan, atau akses yang tidak sah/melanggar hukum.

Praktik keamanan yang direkomendasikan mencakup penerapan dan pemeliharaan Sistem Pengelolaan Keamanan Informasi seperti yang dijelaskan dalam ISO/IEC 27001 serta memastikan aplikasi atau layanan web Anda andal dan bebas dari masalah keamanan umum sebagaimana dijelaskan dalam OWASP Top 10.

Bergantung pada API yang diakses serta jumlah izin pengguna atau pengguna, kami akan mewajibkan aplikasi atau layanan Anda menjalani penilaian keamanan berkala dan mendapatkan Surat Penilaian dari pihak ketiga yang ditunjuk jika produk Anda mentransfer data dari perangkat milik pengguna.

Untuk informasi selengkapnya tentang persyaratan aplikasi yang terhubung ke Health Connect, lihat artikel bantuan ini.

Layanan VPN

VpnService adalah class dasar yang dapat digunakan aplikasi untuk memperluas dan membuat solusi VPN-nya sendiri. Hanya aplikasi yang menggunakan VpnService dan memiliki fungsi inti sebagai VPN dapat membuat tunnel level perangkat yang aman ke server jarak jauh. Pengecualian ini mencakup aplikasi yang memerlukan server jarak jauh untuk fungsi inti seperti:

- Aplikasi kontrol orang tua dan pengelolaan perusahaan.
- Pelacakan penggunaan aplikasi.
- Aplikasi keamanan perangkat (misalnya, anti-virus, pengelolaan perangkat seluler, firewall).
- Alat terkait jaringan (misalnya, akses jarak jauh).
- Aplikasi penjelajahan web.
- Aplikasi operator yang memerlukan penggunaan fungsi VPN untuk menyediakan layanan telepon atau konektivitas.

VpnService tidak dapat digunakan untuk:

- Mengumpulkan data pengguna yang bersifat pribadi dan sensitif tanpa izin dan pengungkapan yang jelas.
- Mengarahkan atau memanipulasi traffic pengguna dari aplikasi lain di perangkat untuk tujuan monetisasi (misalnya, mengalihkan traffic iklan melalui negara yang berbeda dengan negara pengguna).
- Memanipulasi iklan yang dapat memengaruhi monetisasi aplikasi.

Aplikasi yang menggunakan VpnService harus:

- Mendokumentasikan penggunaan VpnService dalam listingan Google Play, dan
- Harus mengenkripsi data dari perangkat ke titik akhir tunnel VPN, dan
- Mematuhi semua Kebijakan Program Developer termasuk kebijakan Penipuan Iklan, Izin, dan Malware.

Berlaku mulai 31 Juli 2023

Izin Alarm yang Tepat

Sebuah izin baru, USE_EXACT_ALARM, akan diperkenalkan. Izin ini memberikan akses ke fungsi alarm yang tepat di aplikasi mulai dari Android 13 (level target API 33).

USE_EXACT_ALARM adalah izin terbatas dan aplikasi hanya boleh mendeklarasikan izin ini apabila fungsi inti aplikasi tersebut mendukung kebutuhan terhadap alarm yang tepat. Aplikasi yang meminta izin terbatas ini akan ditinjau, dan yang tidak memenuhi kriteria penggunaan yang dapat diterima tidak boleh dipublikasikan di Google Play.

Penggunaan yang dapat diterima untuk menggunakan Izin Alarm yang Tepat

Aplikasi Anda hanya boleh menggunakan fungsi USE_EXACT_ALARM saat fungsi inti aplikasi, yaitu yang dapat diakses pengguna, memerlukan tindakan tepat waktu, seperti:

- Aplikasi merupakan alarm atau aplikasi timer.
- Aplikasi merupakan aplikasi kalender yang menampilkan notifikasi acara.

Jika kasus penggunaan Anda untuk fungsi alarm yang tepat tidak disebutkan di atas, sebaiknya lakukan evaluasi untuk mencari tahu apakah Anda dapat menggunakan SCHEDULE_EXACT_ALARM sebagai alternatif.

Untuk informasi selengkapnya tentang fungsi alarm yang tepat, lihat panduan developer 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 selain Google Play. Pembatasan ini tidak berlaku untuk kode yang dijalankan di mesin virtual atau penafsir yang menyediakan akses tidak langsung ke Android API (seperti JavaScript di webview atau browser).

Aplikasi atau kode pihak ketiga (misalnya SDK) dengan bahasa yang ditafsirkan (JavaScript, Python, Lua, dll.) yang dimuat pada runtime (misalnya tidak dikemas dengan aplikasi) tidak boleh mendukung potensi pelanggaran kebijakan Google Play.

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.

Flag Secure Requirements

FLAG_SECURE adalah tanda tampilan layar yang dideklarasikan dalam kode aplikasi untuk menunjukkan bahwa UI-nya berisi data sensitif yang dibatasi pada permukaan aman sambil menggunakan aplikasi tersebut. Tanda ini dirancang untuk mencegah data muncul di screenshot atau dilihat pada layar yang tidak aman. Developer mendeklarasikan tanda ini saat konten aplikasi tidak boleh disiarkan, dilihat, atau dikirimkan ke luar aplikasi atau perangkat pengguna.

Untuk tujuan keamanan dan privasi, semua aplikasi yang didistribusikan di Google Play wajib menghormati deklarasi FLAG_SECURE aplikasi lain. Artinya, aplikasi tidak boleh memfasilitasi atau membuat solusi untuk mengabaikan setelan FLAG_SECURE di aplikasi lain.

Aplikasi yang memenuhi syarat sebagai Alat Aksesibilitas dikecualikan dari persyaratan ini, selama aplikasi tersebut tidak mengirim, menyimpan, atau menyimpan cache konten yang dilindungi FLAG_SECURE untuk akses di luar perangkat pengguna.

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.

- Aplikasi yang menghalangi atau mengganggu aplikasi lain yang menampilkan iklan.
- Aplikasi untuk mencurangi game yang memengaruhi alur game aplikasi lain.
- Aplikasi yang memfasilitasi atau memberikan petunjuk cara meretas 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 untuk pihak ketiga hanya dapat melakukannya di aplikasi yang merupakan tujuan utama aplikasi yang berhubungan dengan 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 tertaut ke atau memfasilitasi distribusi atau penginstalan software berbahaya.
- Aplikasi atau kode pihak ketiga (misalnya, SDK) yang berisi tampilan web dengan Antarmuka JavaScript tambahan yang memuat konten web yang tidak tepercaya (misalnya, URL http://) atau URL yang belum diverifikasi dari sumber yang tidak tepercaya (misalnya, URL yang diperoleh dengan Intent yang tidak tepercaya).

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 seizin pengguna, serta dapat dikembalikan ke setelan semula oleh pengguna.

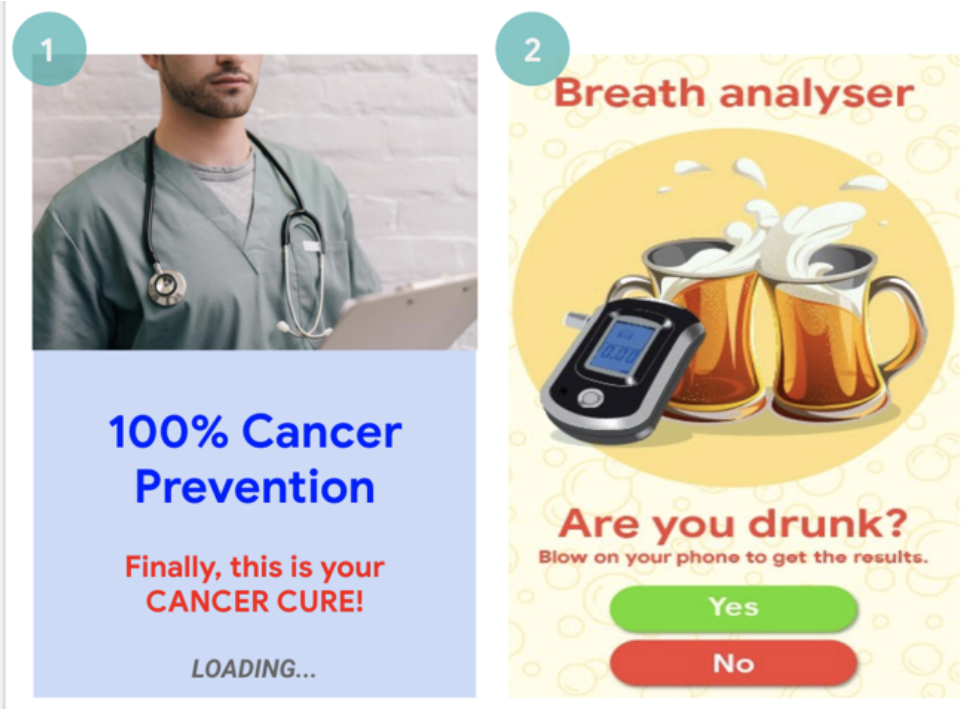
Klaim Menyesatkan

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

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.

- Aplikasi yang memberikan pernyataan tidak benar tentang, atau tidak dengan 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.
- Aplikasi yang mengklaim fungsi yang tidak mungkin diimplementasikan, seperti aplikasi pembasmi serangga, meskipun digambarkan sebagai prank, palsu, candaan, dll.

- Aplikasi yang dikategorikan dengan tidak benar termasuk, tetapi tidak terbatas pada, rating aplikasi atau kategori aplikasi.
- Konten yang terbukti menipu dan salah yang 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 Anda) sebagai alat tes kadar alkohol melalui napas.

Perubahan pada Setelan Perangkat yang 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.

Memperbolehkan Perilaku yang 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, rekening bank, dan surat izin mengemudi. 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 "prank", "untuk tujuan hiburan" (atau sinonim lainnya) tidak akan membebaskan aplikasi dari penerapan kebijakan kami.

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.

- 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 memperbarui 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 mendownload.

Media yang Dimanipulasi

Kami tidak mengizinkan aplikasi yang memberikan atau membantu membuat informasi atau klaim yang menyesatkan atau palsu yang disampaikan melalui citra, 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 satir yang jelas atau parodi.

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.

- 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.

Kebijakan API Level Target Google Play

Untuk memberi pengguna pengalaman yang aman dan terlindungi, Google Play mewajibkan API level target berikut untuk **semua aplikasi**:

Aplikasi baru dan update aplikasi HARUS menargetkan API level Android dalam rentang waktu satu tahun sejak dirilisnya versi Android utama terbaru. Aplikasi baru dan update aplikasi yang gagal memenuhi persyaratan ini tidak akan dapat mengirimkan aplikasi ke Konsol Play.

Aplikasi Google Play yang sudah ada, tidak diupdate, dan tidak menargetkan API level dalam rentang waktu dua tahun sejak dirilisnya versi Android utama terbaru, tidak akan tersedia bagi pengguna baru yang perangkatnya menjalankan versi Android OS lebih baru. Pengguna yang sebelumnya telah menginstal aplikasi ini dari Google Play akan tetap bisa menemukan, menginstal ulang, dan menggunakannya di versi Android OS apa pun yang didukung aplikasi tersebut.

Untuk mendapatkan saran teknis mengenai cara memenuhi persyaratan API level target, harap pelajari panduan migrasi .

Untuk mengetahui linimasa persisnya, harap baca artikel Pusat Bantuan ini.

Malware

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

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 beragam kategori seperti trojan, phishing, serta aplikasi spyware, dan kami akan terus memperbarui dan menambahkan kategori baru.

Meskipun jenis dan kemampuannya bervariasi, malware biasanya memiliki salah satu dari 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 mengakibatkan 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 yang tidak digunakan lagi untuk menjalankan perilaku berbahaya. Namun, perangkat yang masih menjalankan versi Android 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 mendapatkan informasi selengkapnya.

Backdoor (Pintu belakang)

Kode yang dieksekusi di perangkat sehingga memungkinkan operasi jarak jauh yang tidak diinginkan dan berpotensi membahayakan.

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 persetujuan, atau mencoba untuk menyamarkan aktivitas SMS-nya dengan menyembunyikan perjanjian pengungkapan atau pesan SMS dari operator seluler yang memberi tahu pengguna terkait penagihan 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, membuatnya tidak dapat dibaca, dan ada kalanya menyembunyikan pesan SMS dari operator seluler yang menginformasikan pengguna terkait tagihan atau konfirmasi langganan.

Penipuan Telepon
Kode yang membebankan biaya kepada pengguna dengan melakukan panggilan ke nomor premium tanpa persetujuan pengguna.

Penipuan Pulsa
Kode yang mengelabui pengguna agar berlangganan atau membeli konten melalui tagihan telepon selulernya.

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 untuk mencegah pengguna menyadari transaksi finansial yang terjadi.

Berlaku mulai 15 Februari 2023

Stalkerware

Kode yang mengumpulkan data pengguna yang bersifat pribadi atau sensitif dari perangkat dan mentransmisikan data kepada pihak ketiga (perusahaan atau individu lain) untuk tujuan pemantauan.

Aplikasi harus menyediakan pengungkapan yang jelas dan memadai serta mendapatkan persetujuan seperti yang diwajibkan oleh Kebijakan Data Pengguna .

Panduan untuk Aplikasi Pemantauan

Aplikasi yang secara eksklusif dirancang dan dipasarkan untuk memantau individu lain, seperti orang tua yang memantau anak-anaknya atau pengelola perusahaan yang memantau setiap karyawan, adalah aplikasi pemantauan yang diterima asalkan aplikasi pemantauan tersebut sepenuhnya mematuhi persyaratan yang dijelaskan di bawah ini. Aplikasi ini tidak dapat digunakan untuk melacak orang lain (misalnya pasangan) bahkan dengan sepengetahuan dan izin dari orang tersebut, meskipun notifikasi persisten ditampilkan. Aplikasi ini harus menggunakan flag metadata IsMonitoringTool di file manifesnya agar ditandai dengan tepat sebagai aplikasi pemantauan.

Aplikasi pemantauan harus mematuhi persyaratan berikut:

- Aplikasi tidak boleh berfungsi sebagai alat untuk memata-matai atau melakukan pengintaian rahasia.
- Aplikasi tidak boleh menyembunyikan atau menyelubungkan perilaku pelacakan, atau berupaya untuk menyesatkan pengguna terkait fungsi tersebut.
- Aplikasi harus terus memberikan notifikasi persisten kepada pengguna setiap kali aplikasi sedang berjalan, serta menyediakan ikon unik yang mengidentifikasi aplikasi secara jelas.

- Aplikasi harus mengungkapkan fungsi pemantauan atau pelacakan di deskripsi Google Play Store.
- Aplikasi dan listingan 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.
- Aplikasi harus mematuhi setiap hukum yang berlaku. Anda sepenuhnya bertanggung jawab untuk menetapkan pemenuhan aspek hukum aplikasi di lokasi targetnya.

Denial of Service (DoS)

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

Misalnya, hal ini dapat terjadi dengan mengirim permintaan HTTP bervolume tinggi untuk membuat pemuatan berlebihan 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 persetujuan 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 menghadang pengiriman kredensial pengguna pada saat transit.

Target umum phising 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 atau 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 utama penggunaannya adalah untuk mengganti pengelolaan perangkat, dapat dikecualikan dari kategori ransomware jika kode memenuhi persyaratan untuk pengelolaan dan penguncian yang aman, serta persyaratan persetujuan 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 berbahaya tidak memberi tahu pengguna bahwa akan melakukan root pada perangkat, atau memberi tahu pengguna terlebih dahulu terkait proses root ini, tetapi juga menjalankan tindakan lain yang berlaku untuk 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 mengirimkan data pribadi dari perangkat tanpa persetujuan atau pemberitahuan yang memadai.

Misalnya, mengirimkan informasi berikut tanpa pengungkapan atau dengan cara yang tidak diharapkan 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 bahwa game tersebut benar-benar hanya 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. Ini bukan berarti bahwa aplikasi berbahaya, tetapi tanpa tinjauan 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).

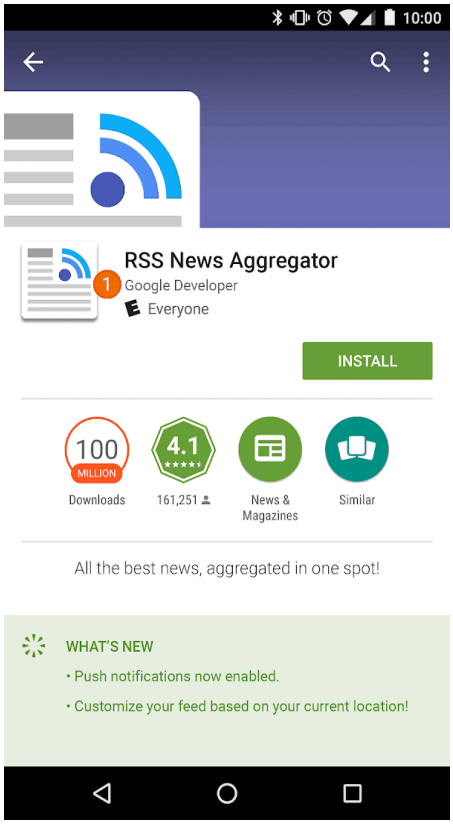
Namun, jika suatu aplikasi memungkinkan eksekusi kode arbitrer dan kami tidak memiliki alasan untuk meyakini bahwa eksekusi kode ini ditambahkan untuk menjalankan perilaku membahayakan, maka aplikasi akan dianggap memiliki kerentanan, bukan malware backdoor (pintu belakang), dan developer akan diminta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

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.

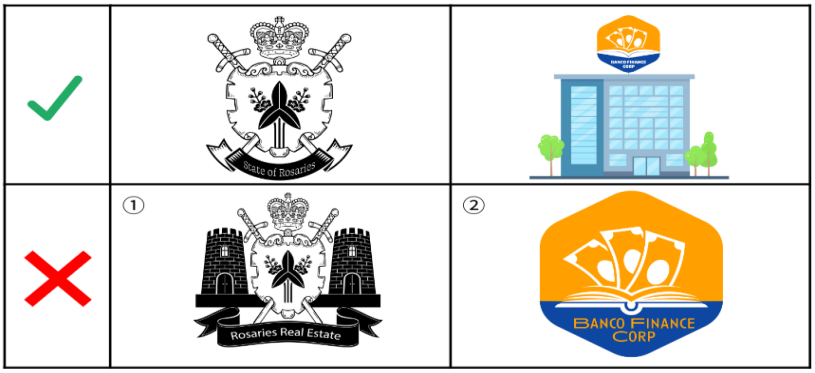
Untuk memastikan bahwa Google Play tetap menjadi platform yang aman dan sopan, kami telah membuat standar yang mendefinisikan dan melarang konten yang berbahaya atau tidak pantas bagi pengguna kami.

- Developer yang secara keliru menyiratkan hubungan dengan perusahaan/developer/entitas/organisasi lain.



① Nama developer yang dicantumkan pada aplikasi ini seolah menunjukkan adanya hubungan resmi dengan Google, padahal kenyataannya tidak demikian.

- Aplikasi yang ikon dan judulnya secara keliru menyiratkan hubungan dengan perusahaan/developer/entitas/organisasi lain.



①Aplikasi menggunakan lambang negara dan menyesatkan pengguna agar percaya bahwa aplikasi tersebut berafiliasi dengan pemerintah.
②Aplikasi menyalin logo entitas bisnis untuk seolah menunjukkan bahwa itu adalah aplikasi bisnis.

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

①Aplikasi menggunakan logo situs mata uang kripto populer di ikon aplikasinya untuk menunjukkan bahwa itu adalah situs resmi.
②Aplikasi menyalin karakter dan judul acara TV terkenal di ikon aplikasinya dan menyesatkan pengguna agar mengira bahwa keduanya berafiliasi dengan acara TV.

- Aplikasi yang mengaku-ngaku sebagai aplikasi resmi entitas ternama. Judul seperti "Justin Bieber Resmi" tidak diperbolehkan tanpa izin atau hak yang diperlukan.
- Aplikasi yang melanggar Pedoman Branding Android .

Mobile Unwanted Software

Di Google, kami yakin jika kami meletakkan 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
- Manipulasi Psikologis

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:

•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

Downloader Berbahaya

Kode yang sebenarnya bukan merupakan software yang tidak diinginkan, tetapi mendownload software yang tidak diinginkan seluler (MUwS) lainnya.

Kode bisa berupa downloader berbahaya jika:

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

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.

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.

- 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.

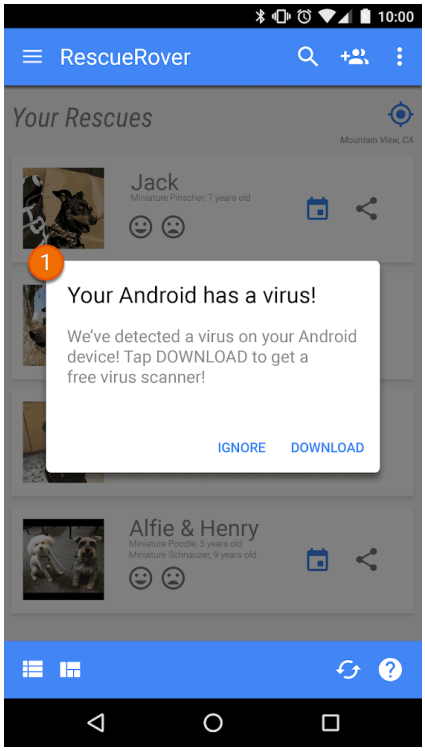
- Pernyataan palsu tentang inventaris iklan oleh aplikasi, misalnya aplikasi yang menginformasikan pada jaringan iklan bahwa aplikasi tersebut berjalan di perangkat iOS padahal sebenarnya berjalan di perangkat Android; aplikasi yang memberikan pernyataan tidak benar tentang nama paket yang dimonetisasi.

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 tingkat 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.

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.

- 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.

Social Engineering

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

Kami tidak mengizinkan aplikasi berisi iklan yang 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 kebijakan terkait iklan perjudian, harap klik di sini.

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

1. Developer yang menagih biaya download aplikasi dari Google Play harus menggunakan sistem penagihan Google Play sebagai metode pembayaran untuk transaksi tersebut.
2. Aplikasi yang didistribusikan melalui Google Play yang mewajibkan atau menerima pembayaran untuk mendapatkan akses ke fitur atau layanan dalam aplikasi, termasuk fungsi aplikasi, konten digital, atau produk digital (secara kolektif disebut "pembelian dalam aplikasi"), harus menggunakan sistem penagihan Google Play untuk transaksi tersebut kecuali Pasal 3 atau Pasal 8 berlaku.

   Contoh layanan atau fitur aplikasi yang mewajibkan penggunaan sistem penagihan Google Play mencakup, tetapi tidak terbatas pada, pembelian dalam aplikasi untuk:

   - Item (seperti mata uang virtual, nyawa tambahan, waktu bermain tambahan, item add-on, karakter, dan avatar);
   - layanan berlangganan (seperti kebugaran, game, kencan, pendidikan, musik, video, upgrade layanan, dan layanan langganan konten lainnya);
   - fungsi atau konten aplikasi (seperti versi aplikasi bebas iklan atau fitur baru yang tidak tersedia dalam versi gratis); dan
   - software dan layanan cloud (seperti layanan penyimpanan data, software produktivitas bisnis, dan software pengelolaan keuangan).

3. Sistem penagihan Google Play tidak boleh digunakan saat:
   a. pembayaran ditujukan terutama:
      - untuk pembelian atau penyewaan produk fisik (seperti bahan makanan, pakaian, peralatan rumah tangga, elektronik);
      - untuk pembelian layanan fisik (seperti layanan transportasi, jasa kebersihan, tiket pesawat, keanggotaan gym, pengiriman makanan, tiket untuk acara langsung); atau
      - sebagai transfer dana untuk melunasi tagihan kartu kredit atau tagihan utilitas (seperti layanan TV kabel dan telekomunikasi);

   b. pembayaran mencakup pembayaran peer-to-peer, lelang online, dan donasi bebas pajak;
   c. pembayaran ditujukan untuk konten atau layanan yang memfasilitasi perjudian online, sebagaimana dijelaskan di bagian Aplikasi Perjudian dalam kebijakan Perjudian, Game, dan Kontes dengan Uang;
   d. pembayaran ditujukan untuk kategori produk apa pun yang dianggap tidak dapat diterima berdasarkan Kebijakan Konten Pusat Pembayaran Google.

   Catatan: Di beberapa pasar, kami menawarkan Google Pay untuk aplikasi yang menjual barang dan/atau layanan fisik. Untuk informasi selengkapnya, buka halaman developer Google Pay.

4. Selain ketentuan yang dijelaskan di Pasal 3 dan Pasal 8, aplikasi tidak boleh mengarahkan pengguna ke metode pembayaran selain sistem penagihan Google Play. Larangan ini mencakup, tetapi tidak terbatas pada, mengarahkan pengguna ke metode pembayaran lain melalui:
   - Listing aplikasi di Google Play;
   - Promosi dalam aplikasi terkait konten yang dapat dibeli;
   - WebView, tombol, link, pesan, iklan, atau pesan ajakan (CTA) lainnya dalam aplikasi; dan
   - Alur antarmuka pengguna dalam aplikasi, termasuk alur pendaftaran atau pembuatan akun, yang mengarahkan pengguna dari aplikasi ke metode pembayaran selain sistem penagihan Google Play sebagai bagian dari alur tersebut.

5. Mata uang virtual hanya boleh digunakan di dalam aplikasi atau untuk game yang dibeli.
6. Developer harus menginformasikan dengan jelas dan akurat kepada pengguna tentang persyaratan dan harga semua aplikasi, langganan, atau fitur dalam aplikasi yang ditawarkan untuk dibeli. Harga dalam aplikasi harus sama dengan harga yang ditampilkan pada antarmuka layanan penagihan Play yang dilihat oleh pengguna. Jika deskripsi produk Anda di Google Play mencantumkan fitur dalam aplikasi yang mungkin memerlukan biaya khusus atau tambahan, listing aplikasi Anda harus menyampaikan dengan jelas kepada pengguna bahwa diperlukan pembayaran untuk mengakses fitur tersebut.
7. Aplikasi dan game yang menawarkan mekanisme untuk menerima item virtual acak dari pembelian, termasuk tetapi tidak terbatas pada "loot box", harus dengan jelas mengungkapkan peluang untuk menerima item tersebut sebelum, dan di saat yang hampir bersamaan dengan, pembelian tersebut.
8. Kecuali jika ketentuan yang dijelaskan di Pasal 3 berlaku, developer aplikasi yang didistribusikan melalui Google Play di ponsel dan tablet yang mewajibkan atau menerima pembayaran dari pengguna di Korea Selatan untuk mendapatkan akses ke pembelian dalam aplikasi dapat menawarkan kepada pengguna sistem penagihan dalam aplikasi selain sistem penagihan Google Play untuk transaksi tersebut jika mereka berhasil melengkapi formulir pernyataan sistem penagihan tambahan dalam aplikasi dan menyetujui persyaratan program dan tambahan yang disertakan di dalamnya.

Catatan: Untuk melihat linimasa dan pertanyaan umum terkait kebijakan ini, harap buka Pusat Bantuan kami.

Kami tidak mengizinkan aplikasi berisi iklan yang 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 kebijakan terkait iklan perjudian, harap klik di sini.

Kami tidak mengizinkan aplikasi berisi iklan yang menipu atau mengganggu. Iklan hanya boleh ditampilkan dalam aplikasi yang menayangkannya. Kami menganggap iklan dan penawaran terkaitnya yang ditayangkan di aplikasi Anda sebagai bagian dari aplikasi Anda. Iklan yang ditampilkan di aplikasi Anda harus mematuhi semua kebijakan kami. Untuk kebijakan terkait iklan perjudian, harap 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:

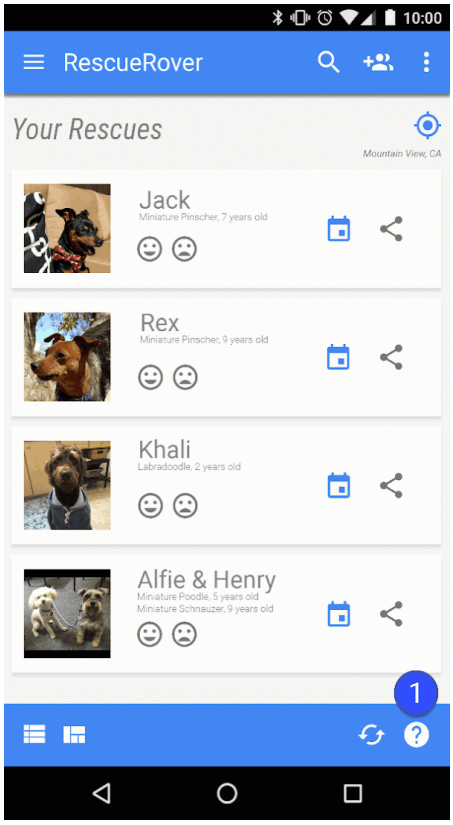
- Penggunaan atau pengumpulan data lokasi perangkat berbasis izin untuk tujuan periklanan harus jelas bagi pengguna dan didokumentasikan dalam kebijakan privasi wajib aplikasi, termasuk penautan ke setiap kebijakan privasi jaringan iklan relevan yang membahas penggunaan data lokasi.
- Sesuai dengan persyaratan Izin Akses Lokasi, izin akses lokasi hanya boleh diminta untuk menerapkan fitur atau layanan saat ini dalam aplikasi Anda, dan tidak boleh meminta izin akses lokasi perangkat hanya untuk penggunaan iklan.

Iklan yang Menipu

Iklan tidak boleh 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.

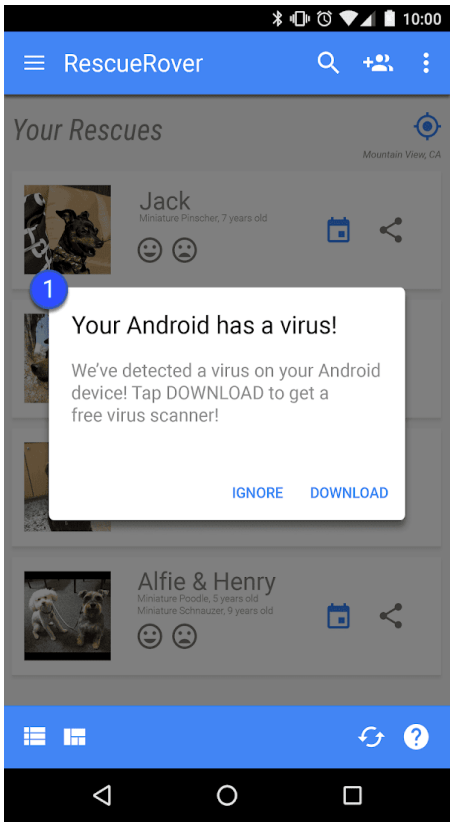
Untuk memastikan bahwa Google Play tetap menjadi platform yang aman dan sopan, kami telah membuat standar yang mendefinisikan dan melarang konten yang berbahaya atau tidak pantas bagi pengguna kami.

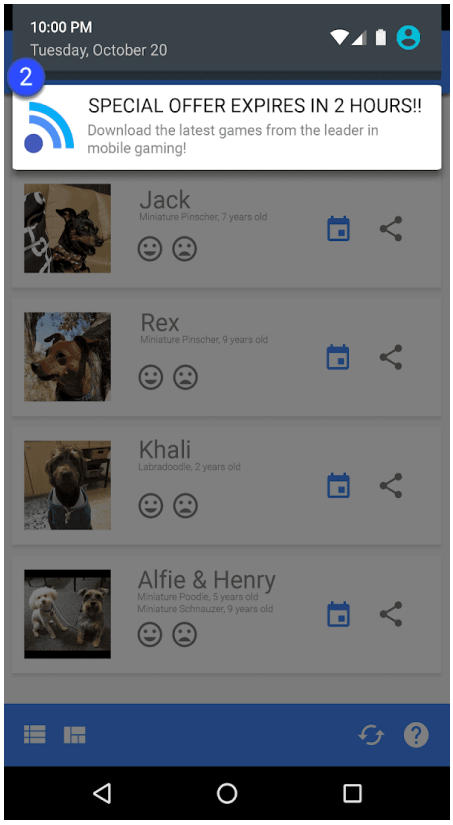
- Iklan yang meniru antarmuka aplikasi:



① Ikon tanda tanya dalam aplikasi ini adalah iklan yang membawa pengguna ke laman landas eksternal.

- Iklan yang meniru notifikasi sistem:





① ② Contoh di atas menggambarkan iklan yang meniru berbagai sistem notifikasi.

Monetisasi Layar Kunci

Aplikasi tidak boleh menampilkan iklan atau fitur yang memonetisasi layar perangkat yang dikunci, kecuali memiliki tujuan khusus untuk berfungsi 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.

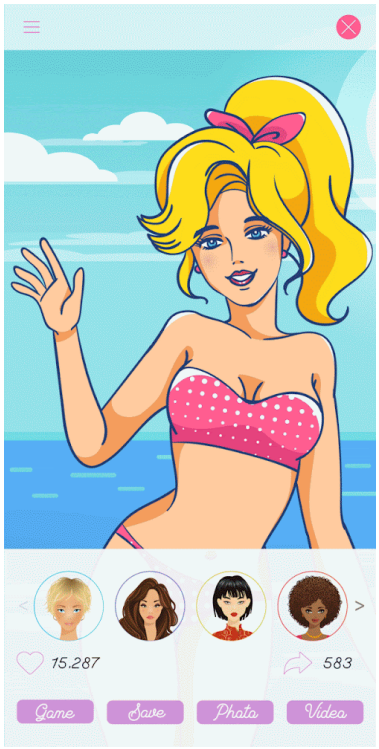
Aplikasi Anda tidak boleh memaksa pengguna agar mengklik iklan atau mengirimkan informasi pribadi untuk tujuan periklanan sebelum mereka dapat sepenuhnya menggunakan aplikasi. Iklan interstisial hanya boleh ditampilkan dalam aplikasi yang menayangkannya. Jika aplikasi Anda menampilkan iklan interstisial atau iklan lain yang mengganggu penggunaan normal, iklan tersebut harus dapat ditutup dengan mudah tanpa konsekuensi.

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.

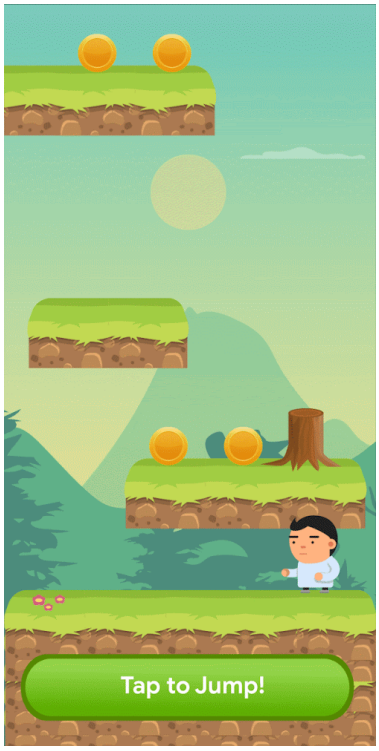
- Iklan yang menutupi seluruh layar atau mengganggu penggunaan normal dan tidak memberikan cara yang jelas untuk menutup iklan:

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



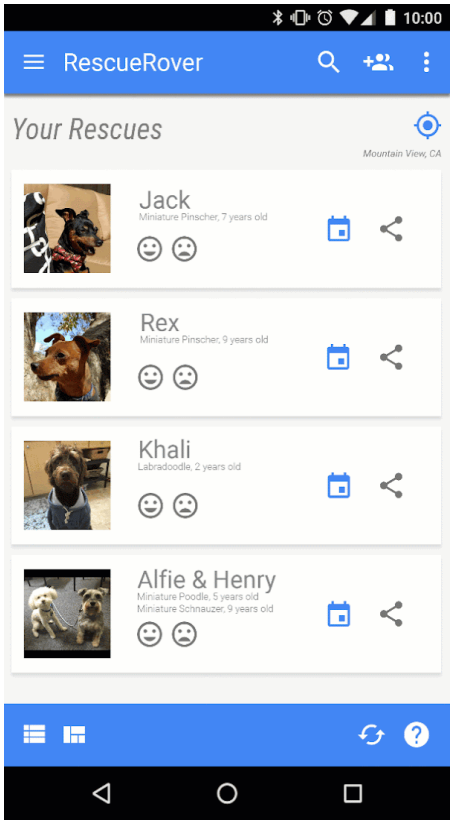
Iklan yang muncul tiba-tiba di area yang biasa diketuk pengguna untuk menggunakan fungsi dalam aplikasi

Mengganggu Aplikasi, Iklan Pihak Ketiga, atau Fungsi Perangkat

Iklan yang terkait dengan aplikasi Anda tidak boleh mengganggu aplikasi, iklan, atau pengoperasian perangkat lain, 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.

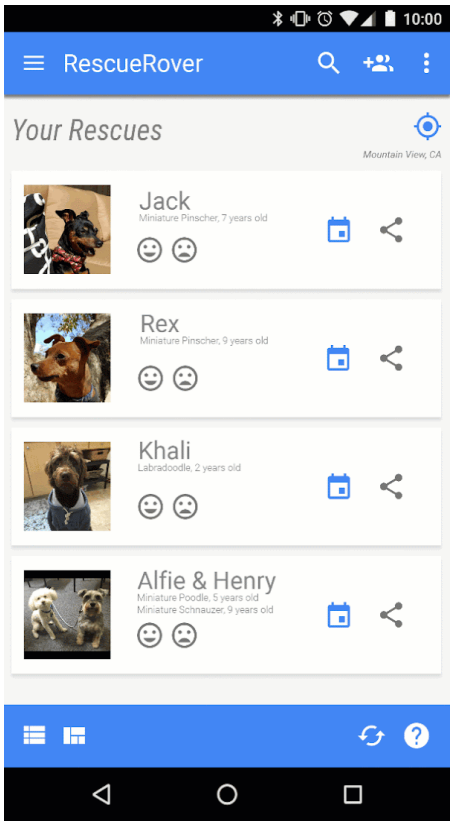
Untuk memastikan bahwa Google Play tetap menjadi platform yang aman dan sopan, kami telah membuat standar yang mendefinisikan dan melarang konten yang berbahaya atau tidak pantas bagi pengguna kami.

- 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:

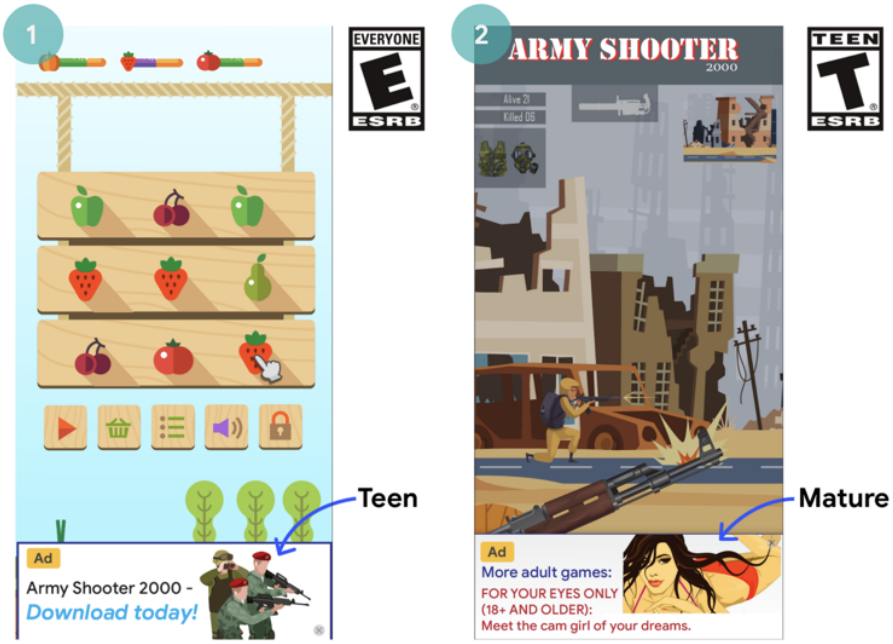


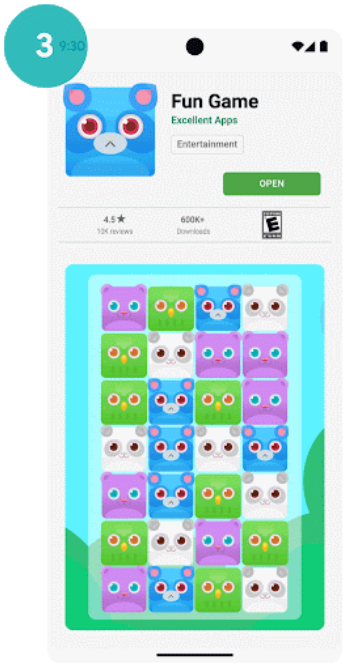
Deskripsi: Pengguna berupaya keluar dari aplikasi dan menavigasi ke layar utama, tetapi alurnya terganggu oleh iklan.

Iklan yang Tidak Pantas

Iklan dan penawaran terkaitnya (misalnya, iklan yang mempromosikan hasil download aplikasi lain) yang ditampilkan dalam aplikasi harus sesuai dengan rating konten aplikasi Anda, meskipun konten itu sendiri sudah sesuai dengan kebijakan kami.

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.





① Iklan ini tidak pantas (Remaja) untuk rating konten aplikasi (Semua Orang)
② Iklan ini tidak pantas (Dewasa) untuk rating konten aplikasi (Remaja)
③ Penawaran iklan (mempromosikan hasil download aplikasi Dewasa) tidak pantas untuk rating konten aplikasi game tempat iklan tersebut ditampilkan (Semua Orang)

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 (AAID) hanya boleh digunakan untuk iklan dan analisis pengguna. Status setelan "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, dst.) untuk tujuan periklanan apa pun. ID iklan hanya boleh dihubungkan dengan informasi identitas pribadi melalui izin eksplisit dari pengguna.
  - Penggunaan analisis: ID Iklan tidak boleh dihubungkan dengan informasi identitas pribadi atau dikaitkan dengan ID perangkat tetap (misalnya: SSAID, alamat MAC, IMEI, dst.) untuk tujuan analisis. Harap baca Kebijakan_Data Pengguna untuk mendapatkan panduan tambahan tentang ID perangkat tetap.
- **Menghormati pilihan pengguna**.
  - Jika reset dilakukan, ID iklan baru tidak boleh dihubungkan ke ID iklan sebelumnya atau data yang berasal dari ID iklan sebelumnya tanpa izin eksplisit dari pengguna.
  - Anda harus mematuhi setelan "Memilih tidak ikut dari Periklanan Menurut Minat" atau "Memilih tidak ikut dari Personalisasi Iklan" pengguna. Jika pengguna telah mengaktifkan setelan ini, Anda tidak dapat menggunakan ID iklan tersebut untuk membuat profil pengguna demi tujuan iklan, atau untuk menargetkan pengguna dengan iklan yang dipersonalisasi. Aktivitas yang diizinkan meliputi pengiklanan kontekstual, pembatasan frekuensi, tracking konversi, pelaporan dan keamanan, serta deteksi penipuan.
  - Di perangkat yang lebih baru, saat pengguna menghapus ID iklan Android, ID tersebut akan dihapus. Setiap upaya yang dilakukan untuk mengakses ID akan memunculkan string berisi banyak angka nol. Perangkat tanpa ID iklan tidak boleh dihubungkan ke data yang ditautkan ke atau berasal dari ID iklan sebelumnya.
- **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 lebih lanjut standar privasi kami, tinjau kebijakan Data Pengguna kami.
- **Mematuhi persyaratan penggunaan**. ID iklan hanya dapat digunakan sesuai dengan Kebijakan Program Developer Google Play, termasuk oleh pihak mana pun yang mungkin berbagi ID ini dengan Anda, 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 iklan apa pun.

Pengalaman Better Ads

Developer wajib mematuhi panduan iklan berikut untuk memastikan pengalaman berkualitas tinggi bagi pengguna saat mereka menggunakan aplikasi Google Play. Iklan Anda tidak boleh ditampilkan kepada pengguna dengan cara yang tidak terduga seperti berikut ini:

- Iklan interstisial layar penuh dari semua format (video, GIF, statis, dll.) yang muncul secara tidak terduga, biasanya saat pengguna telah memilih untuk melakukan aktivitas lain, tidak diizinkan.
  - Iklan yang muncul saat permainan game di awal level atau di awal segmen konten, tidak diizinkan.
  - Iklan interstisial video layar penuh yang muncul sebelum layar pemuatan (layar pembuka) aplikasi tidak diizinkan.
- Iklan interstisial layar penuh dari semua format yang tidak dapat ditutup setelah 15 detik tidak diizinkan. Alih-alih, sebaiknya gunakan interstisial layar penuh, atau interstisial layar penuh yang tidak mengganggu pengguna saat mereka melakukan tindakan (misalnya, setelah layar skor di aplikasi game), dapat ditayangkan selama lebih dari 15 detik.

Kebijakan ini tidak berlaku untuk iklan reward yang secara eksplisit telah dikonfirmasi oleh pengguna untuk mereka tonton (misalnya, iklan yang secara jelas ditawarkan developer kepada pengguna untuk

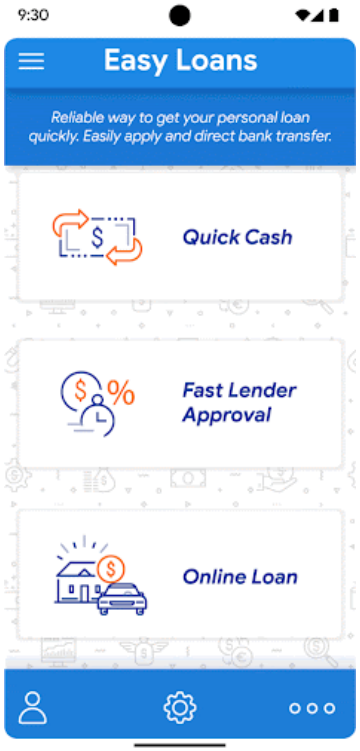
ditonton agar dapat membuka fitur game tertentu atau konten). Kebijakan ini juga tidak berlaku untuk monetisasi dan iklan yang tidak mengganggu penggunaan normal aplikasi atau permainan game (misalnya, konten video dengan iklan terintegrasi, iklan banner yang bukan layar penuh).

Panduan ini terinspirasi dari panduan Better Ads Standards - Pengalaman Aplikasi Seluler . Untuk informasi selengkapnya mengenai Better Ads Standards, buka Coalition for Better Ads .

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.

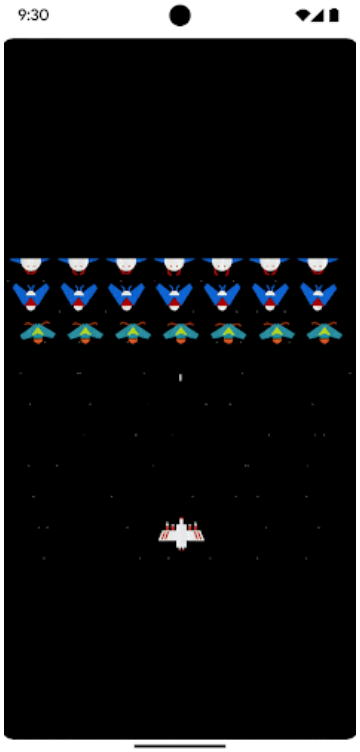
- Iklan tidak terduga yang muncul selama permainan game atau segmen konten (misalnya, setelah pengguna mengklik tombol, dan sebelum tindakan akibat klik tombol diterapkan). Iklan ini tidak diduga oleh pengguna, karena pengguna berharap memulai game atau terlibat dalam konten.

① Iklan statis yang tidak terduga muncul selama permainan game di awal level.



② Iklan video yang tidak terduga muncul selama awal segmen konten.

- Iklan layar penuh yang muncul selama permainan game dan tidak dapat ditutup setelah 15 detik.



① Iklan interstisial muncul selama permainan game, dan tidak menawarkan opsi kepada pengguna untuk melewati iklan dalam 15 detik.

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. Kami tidak mengizinkan aplikasi yang membuat pengguna

merasakan pengalaman pembelian yang menipu atau manipulatif (termasuk pembelian atau langganan dalam aplikasi).

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

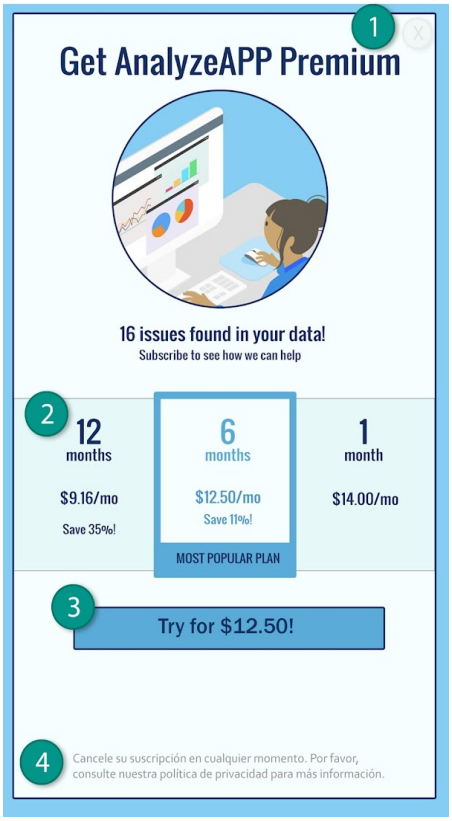
Langganan harus memberikan nilai berkelanjutan atau berulang kepada pengguna sepanjang masa berlaku langganan, dan tidak boleh digunakan untuk menawarkan manfaat satu kali pakai yang efektif kepada pengguna (misalnya, SKU yang menyediakan kredit/mata uang dalam aplikasi sekaligus, atau booster game sekali pakai). Langganan Anda mungkin menawarkan bonus promosi atau insentif, tetapi hal ini hanyalah sebagai pelengkap nilai berkelanjutan atau berulang yang diberikan sepanjang masa berlaku langganan**.** Produk yang tidak menawarkan nilai berkelanjutan dan berulang harus menggunakan produk dalam aplikasi, bukan produk langganan.

Anda tidak boleh menyamarkan atau salah mengartikan manfaat satu kali pakai kepada pengguna sebagai langganan. Hal ini termasuk memodifikasi langganan untuk mengubahnya menjadi penawaran satu kali pakai (misalnya, membatalkan, menghentikan penggunaan, atau meminimalkan nilai berulang) setelah pengguna membeli langganan.

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.

- 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" atau "Coba Langganan premium - 3 hari secara gratis", untuk langganan dengan biaya berulang otomatis.
- Beberapa layar dalam alur pembelian yang mengarahkan pengguna untuk mengklik tombol berlangganan secara tidak sengaja.
- Langganan yang tidak menawarkan nilai berkelanjutan atau berulang — misalnya, menawarkan 1.000 permata untuk bulan pertama, kemudian menguranginya menjadi 1 permata di bulan-bulan berikutnya.
- Mengharuskan pengguna untuk mendaftar ke perpanjangan otomatis langganan guna memberikan manfaat satu kali pakai, dan membatalkan langganan pengguna tanpa permintaan mereka setelah pembelian.

Contoh 1:



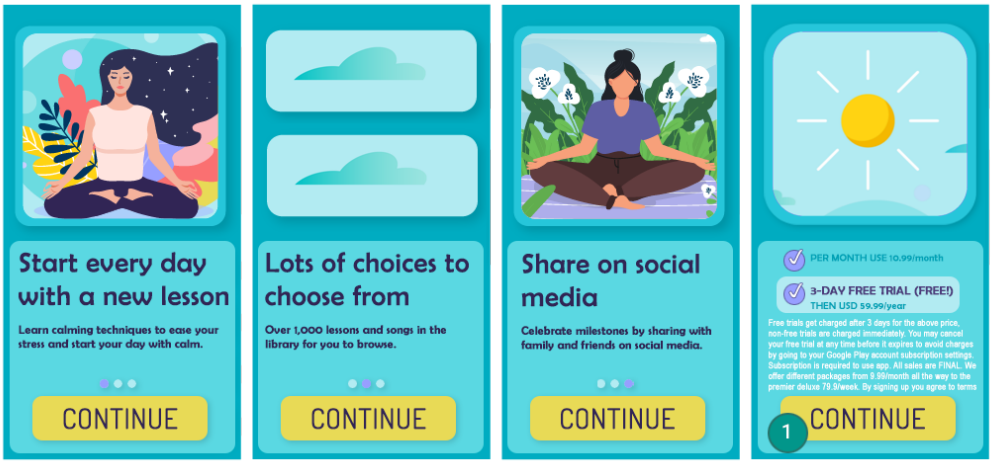
① Tombol tolak tidak terlihat jelas dan pengguna mungkin tidak memahami bahwa fungsi aplikasi dapat diakses tanpa perlu menerima penawaran langganan.

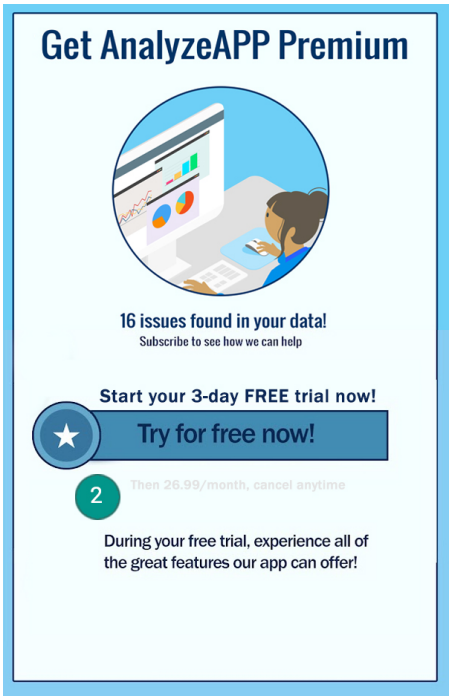
② Penawaran hanya menampilkan harga yang berkaitan dengan biaya bulanan, dan pengguna mungkin tidak mengetahui jika akan dikenai biaya setara dengan enam bulan langganan ketika berlangganan.

③ Penawaran hanya menampilkan harga perkenalan, dan pengguna mungkin tidak mengetahui bahwa mereka akan otomatis dikenai biaya pada akhir periode perkenalan.

④ Penawaran seharusnya dilokalkan dalam bahasa yang sama dengan yang digunakan pada persyaratan dan ketentuan sehingga pengguna dapat memahami keseluruhan penawaran.

Contoh 2:





① Klik berulang di area tombol yang sama menyebabkan pengguna secara tidak sengaja mengklik tombol "lanjutkan" terakhir untuk berlangganan.

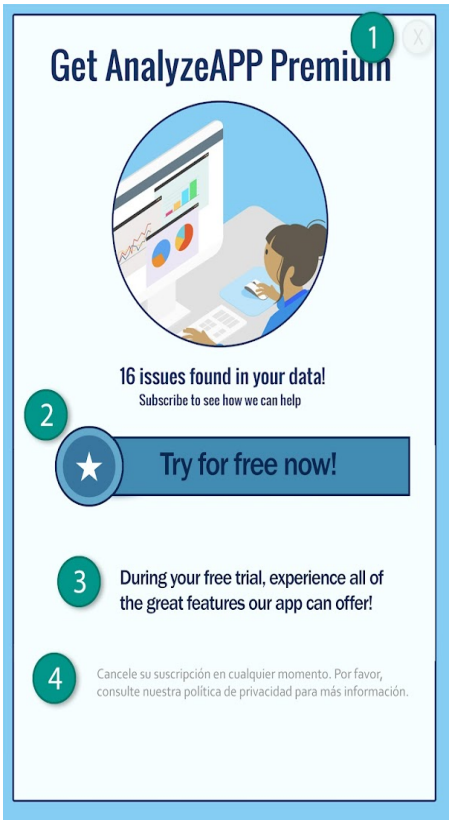
② Jumlah yang akan dibebankan kepada pengguna di akhir masa uji coba sulit untuk dibaca, sehingga pengguna mungkin berpikir bahwa paket tersebut gratis

Uji Coba Gratis & Penawaran Harga Perkenalan

Sebelum pengguna terdaftar di langganan: Anda harus menerangkan persyaratan penawaran secara 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 diubah menjadi langganan berbayar, berapa biaya langganan berbayar, dan bahwa pengguna dapat membatalkan langganan tersebut jika mereka tidak ingin mengubahnya menjadi langganan berbayar.

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.

- Penawaran yang tidak memberi tahu dengan jelas tentang durasi uji coba gratis atau harga perkenalan.
- 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.



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 & Pengembalian Dana Langganan

Jika Anda menjual langganan di aplikasi Anda, Anda harus memastikan bahwa aplikasi Anda mengungkapkan dengan jelas bagaimana pengguna dapat mengelola atau membatalkan langganan mereka. Anda juga harus menyertakan akses ke metode online untuk membatalkan langganan dalam aplikasi Anda. Di setelan akun aplikasi Anda (atau halaman yang setara), Anda dapat memenuhi persyaratan ini dengan menyertakan:

- Link ke Pusat Langganan Google Play (untuk aplikasi yang menggunakan sistem penagihan Google Play); dan/atau
- akses langsung ke proses pembatalan Anda.

Jika pengguna membatalkan langganan yang dibeli melalui sistem penagihan Google Play, kebijakan umum kami adalah bahwa pengguna tidak akan menerima pengembalian dana untuk periode penagihan aktif, tetapi akan terus menerima konten langganan mereka selama sisa periode penagihan aktif, terlepas dari tanggal pembatalan. Pembatalan pengguna akan berlaku setelah periode penagihan aktif berlalu.

Anda (sebagai penyedia konten atau akses) dapat menerapkan kebijakan pengembalian dana yang lebih fleksibel kepada pengguna secara langsung. 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.

Program SDK Iklan Tersertifikasi Mandiri Keluarga

Jika Anda menayangkan iklan dalam aplikasi, dan satu-satunya target audiens Anda adalah anak-anak seperti yang dijelaskan dalam Kebijakan Keluarga , Anda hanya boleh menggunakan SDK iklan yang memiliki kepatuhan tersertifikasi mandiri dengan kebijakan Google Play, termasuk Persyaratan Tersertifikasi Mandiri SDK Iklan di bawah ini.

Jika target audiens untuk aplikasi adalah anak-anak dan pengguna dewasa, Anda harus memastikan bahwa iklan yang ditampilkan kepada anak-anak secara eksklusif berasal dari salah satu SDK iklan ini (misalnya, melalui penggunaan langkah-langkah verifikasi usia). Aplikasi dalam program Didesain untuk Keluarga diwajibkan untuk hanya menggunakan SDK iklan tersertifikasi mandiri.

Perlu diperhatikan bahwa Anda bertanggung jawab untuk memastikan bahwa semua versi SDK yang diimplementasikan di aplikasi, termasuk SDK Iklan Tersertifikasi Mandiri, mematuhi semua kebijakan, hukum dan peraturan setempat yang berlaku. Google tidak memberikan pernyataan atau jaminan mengenai keakuratan informasi yang diberikan SDK iklan selama proses sertifikasi mandiri.

Penggunaan SDK iklan tersertifikasi mandiri Keluarga hanya diperlukan 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 Google 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 SDK Iklan Tersertifikasi Mandiri Keluarga

- Mendefinisikan apa yang dimaksud dengan perilaku dan konten 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 Google 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 mengirimkan pengujian aplikasi dan informasi yang ditunjukan pada formulir minat di bawah, untuk memverifikasi kepatuhan terhadap kebijakan SDK iklan dengan semua persyaratan sertifikasi mandiri dan merespons setiap permintaan informasi selanjutnya secara tepat waktu, seperti mengirim rilis versi baru untuk memverifikasi kepatuhan versi SDK iklan terhadap semua persyaratan sertifikasi mandiri.

- Sertifikasi mandiri bahwa semua rilis versi baru mematuhi Kebijakan Program Developer Google Play terbaru, Termasuk Persyaratan Kebijakan Keluarga.

Catatan: Tersertifikasi Mandiri Keluarga SDK Iklan harus mendukung penayangan iklan yang mematuhi hukum dan peraturan yang relevan terkait anak-anak, yang mungkin berlaku bagi penayangnya.

Berikut adalah persyaratan mediasi untuk platform penayangan saat menayangkan iklan kepada anak-anak:

- Hanya menggunakan SDK Iklan Tersertifikasi Mandiri Keluarga 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 Keluarga di sini .

Selain itu, developer dapat membagikan formulir minat ini dengan SDK iklan yang diharapkan untuk sertifikasi mandiri.

Listingan Play Store dan Promosi

Promosi dan visibilitas aplikasi Anda sangat memengaruhi kualitas toko. Jangan membuat listingan Play Store yang berisi spam, promosi berkualitas rendah, dan 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 (seperti iklan) yang menipu atau merugikan pengguna atau ekosistem developer. Praktik promosi menipu atau berbahaya jika perilaku atau kontennya melanggar Kebijakan Program Developer kami.

Contoh pelanggaran umum:

- Menggunakan iklan yang menipu di situs, aplikasi, atau properti lainnya, termasuk notifikasi yang mirip dengan notifikasi dan peringatan sistem.
- Menggunakan iklan seksual vulgar guna mengarahkan pengguna ke listingan Google Play aplikasi Anda untuk didownload.
- 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 semua jaringan iklan, afiliasi, atau iklan yang terkait dengan aplikasi Anda mematuhi kebijakan ini.

Metadata

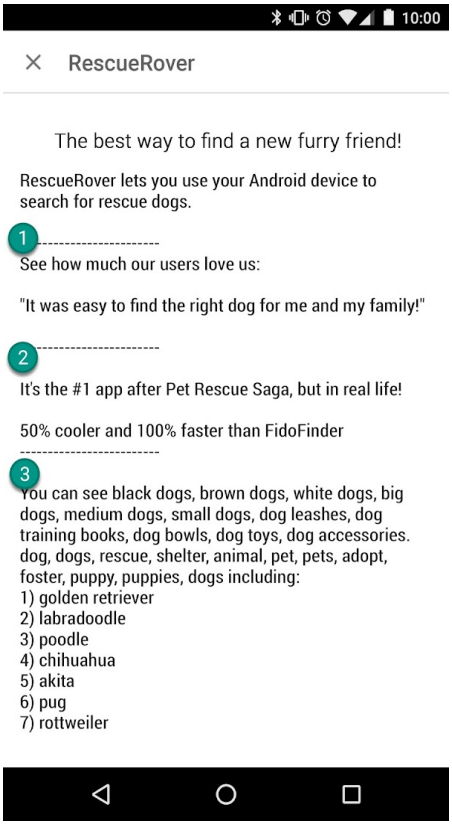
Kami melarang aplikasi dengan metadata yang menyesatkan, salah format, non-deskriptif, tidak relevan, berlebihan, atau tidak pantas, termasuk, tetapi tidak terbatas pada, deskripsi aplikasi, nama developer, judul, ikon, screenshot, dan gambar promosi. Developer harus memberikan deskripsi aplikasi yang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

Nama developer, ikon, dan judul aplikasi Anda sangat berguna bagi pengguna untuk menemukan dan mempelajari aplikasi Anda. Jangan gunakan emoji, emotikon, atau karakter khusus berulang dalam elemen metadata ini. Hindari penggunaan HURUF BESAR SEMUANYA kecuali jika ini adalah bagian dari

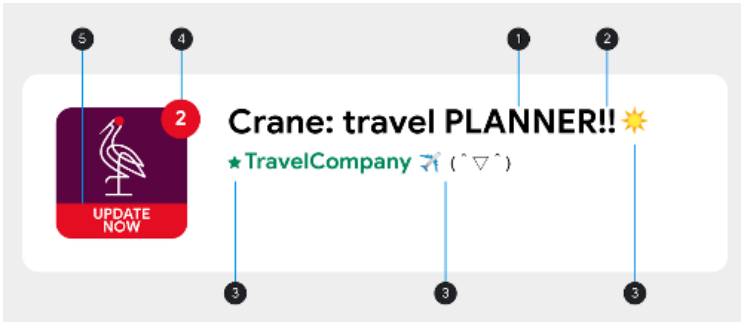
nama merek Anda. Simbol menyesatkan di ikon aplikasi tidak diizinkan, misalnya: indikator titik pesan baru saat tidak ada pesan baru dan simbol download/instal saat aplikasi tidak terkait dengan konten yang didownload. Judul aplikasi Anda harus berisi maksimal 30 karakter.

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

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.



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



① HURUF BESAR SEMUANYA meskipun bukan bagian dari nama merek
② Urutan karakter khusus yang tidak relevan dengan aplikasi
③ Penggunaan emoji, emotikon (termasuk kaomoji), dan karakter khusus
④ Simbol yang menyesatkan
⑤ Teks yang menyesatkan

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

- Citra atau video dengan konten yang menggoda secara seksual. Hindari gambar menjurus 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, IPTEK, atau Seni) juga harus sesuai untuk segala umur dalam listingan Play Store.

Berikut beberapa praktik terbaik:

- Tonjolkan keunggulan aplikasi Anda. Bagikan fakta menarik dan unik tentang aplikasi Anda agar pengguna memahami keistimewaan aplikasi Anda.
- 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.

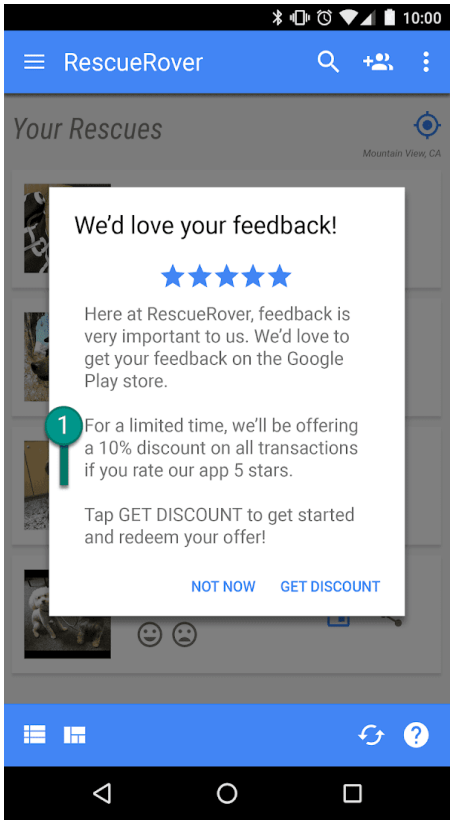
Rating, Ulasan, dan Penginstalan Pengguna

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. Instal, ulasan, dan rating yang disebabkan adanya insentif mencakup penggunaan teks atau gambar di nama developer, ikon, dan judul aplikasi Anda yang menunjukkan harga atau informasi promosi lainnya.

Developer tidak boleh menambahkan teks atau gambar yang menunjukkan performa atau peringkat aplikasi di Play Store, atau menyarankan hubungan dengan program Google Play yang sudah ada di nama developer, ikon, atau judul aplikasi.

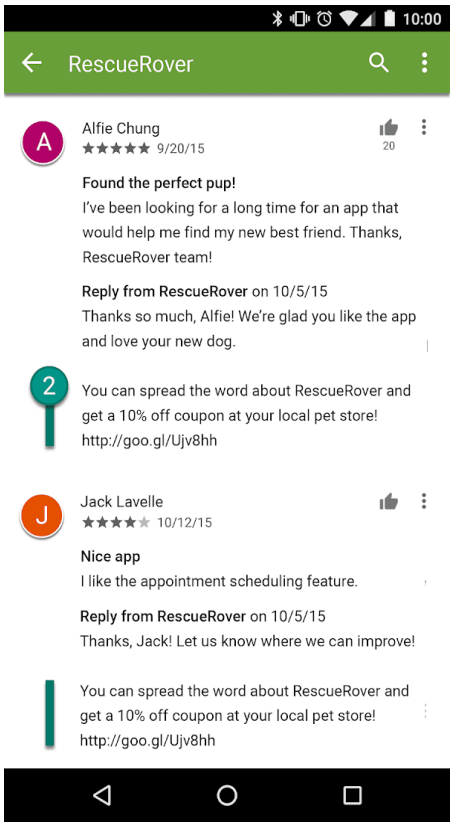
Untuk memastikan bahwa Google Play tetap menjadi platform yang aman dan sopan, kami telah membuat standar yang mendefinisikan dan melarang konten yang berbahaya atau tidak pantas bagi pengguna kami.

- Meminta pengguna memberi rating aplikasi Anda dan menawarkan insentif:



① Notifikasi ini menawarkan diskon kepada pengguna asalkan mereka memberi rating yang tinggi.

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



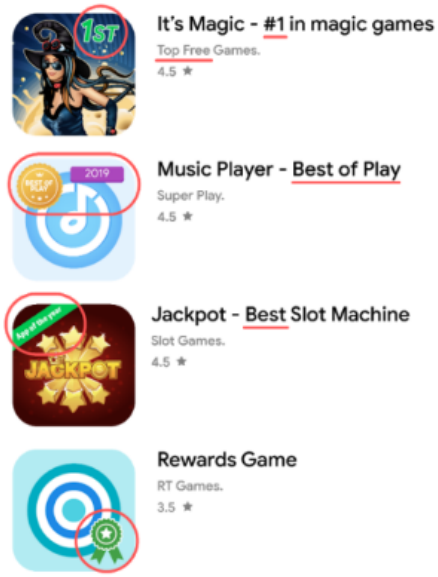
② Ulasan ini mendorong pengguna untuk mempromosikan aplikasi RescueRover dengan menawarkan kupon.

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

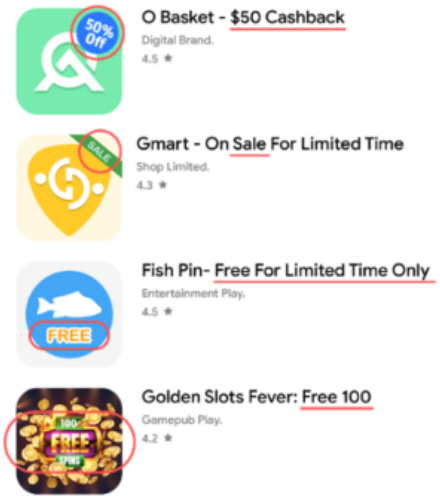
- Buat balasan Anda tetap fokus pada masalah dalam komentar pengguna dan jangan meminta rating lebih tinggi.
- Sertakan referensi yang berguna, seperti URL dukungan atau halaman FAQ.

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.

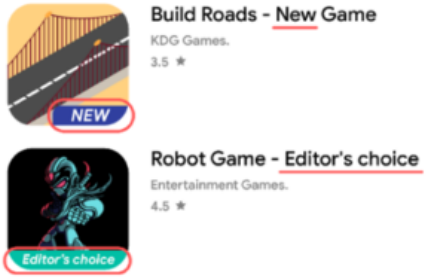
- Gambar atau teks yang menunjukkan performa atau peringkat aplikasi di Play Store, seperti 'Aplikasi terbaik tahun ini', '#1', 'Terbaik di Play 20XX', 'Populer', ikon penghargaan, dll.



- Gambar atau teks yang menunjukkan informasi harga dan promosi, seperti 'Diskon 10%', 'cash back $50', 'gratis hanya untuk waktu terbatas', dll.



- Gambar atau teks yang menunjukkan program Google Play, seperti 'Pilihan editor', 'Baru', dll.



Rating Konten

Rating konten di Google Play diberikan 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.

Cara konten rating digunakan

Rating konten digunakan untuk memberi tahu konsumen, terutama orang tua, tentang potensi konten tidak pantas yang ada dalam aplikasi. Rating konten juga membantu 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.

Cara konten rating ditetapkan

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. Representasi konten aplikasi yang keliru dapat menyebabkan aplikasi Anda dihapus atau ditangguhkan, jadi sangatlah penting untuk memberikan respons yang akurat saat mengisi kuesioner rating konten.

Untuk mencegah aplikasi agar tidak dicantumkan sebagai “Belum diberi rating”, Anda harus melengkapi kuesioner rating konten untuk setiap aplikasi baru yang dikirim ke Konsol Play, serta untuk semua aplikasi yang sudah ada dan aktif di Google Play. Aplikasi tanpa rating konten akan dihapus dari Play Store.

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 mencari tahu informasi selengkapnya mengenai otoritas rating dan cara melengkapi kuesioner rating konten.

Banding 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 Berita adalah aplikasi yang:

- Dideklarasikan sebagai aplikasi "Berita" di Konsol Google Play, atau
- Dikelompokkan dalam kategori “Berita dan Majalah” di Google Play Store serta dideskripsikan sebagai aplikasi “berita” dalam judul aplikasi, ikon, nama developer, atau deskripsinya.

Contoh aplikasi dalam kategori “Berita dan Majalah” yang memenuhi syarat sebagai aplikasi Berita:

- Aplikasi yang dideskripsikan sebagai aplikasi “berita” dalam deskripsi aplikasi, termasuk namun tidak terbatas pada:
  - Berita terkini
  - Koran
  - Berita terbaru
  - Berita lokal
  - Berita harian
- Aplikasi yang memiliki kata “Berita” dalam nama developer, ikon, atau judul aplikasi.

Namun, jika aplikasi yang utamanya berisi konten buatan pengguna (mis., aplikasi media sosial), aplikasi tersebut tidak boleh dideklarasikan sebagai aplikasi Berita, dan tidak dianggap sebagai aplikasi Berita.

Aplikasi Berita yang mewajibkan pengguna membeli langganan harus menyediakan pratinjau konten dalam aplikasi untuk pengguna sebelum mereka membelinya.

Aplikasi Berita harus:

- Memberikan informasi kepemilikan tentang aplikasi dan sumber artikel berita termasuk, tetapi tidak terbatas pada, penerbit atau penulis asli setiap artikel. Jika dalam praktiknya aplikasi tidak mencantumkan nama tiap-tiap penulis artikel, aplikasi berita tersebut harus menjadi penerbit asli artikel. Perlu diperhatikan bahwa link ke akun media sosial tidak berlaku sebagai informasi penulis atau penerbit yang memadai.
- Memiliki halaman dalam aplikasi atau situs khusus yang secara jelas berlabel sebagai berisi informasi kontak, mudah ditemukan (mis. ditautkan di bagian bawah halaman beranda atau di menu navigasi situs), serta memberikan informasi kontak penerbit berita yang valid, termasuk alamat email atau nomor telepon kontak. Perlu diperhatikan bahwa link ke akun media sosial tidak berlaku sebagai informasi kontak penerbit yang memadai.

Aplikasi Berita tidak boleh:

- Berisi kesalahan ejaan dan/atau tata bahasa yang signifikan,
- Hanya berisi konten statis (mis., konten yang berusia lebih dari tiga bulan), atau
- Memiliki tujuan utama sebagai marketing afiliasi atau untuk menghasilkan pendapatan iklan.

Perlu diperhatikan bahwa aplikasi Berita *dapat* menggunakan iklan dan bentuk marketing lainnya untuk dimonetisasi, selama tujuan utama aplikasi bukan untuk menjual produk dan layanan atau menghasilkan pendapatan 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.

Harap baca artikel ini untuk mengetahui cara terbaik memberikan informasi yang diperlukan.

Spam dan Minim Fungsi

Setidaknya, aplikasi harus memberikan fungsi dasar dan pengalaman yang layak kepada pengguna. Aplikasi yang tidak bekerja, yang menunjukkan perilaku lain yang tidak 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, misalnya aplikasi yang mengirim pesan tidak diminta kepada pengguna atau yang bersifat pengulangan dan 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.

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.

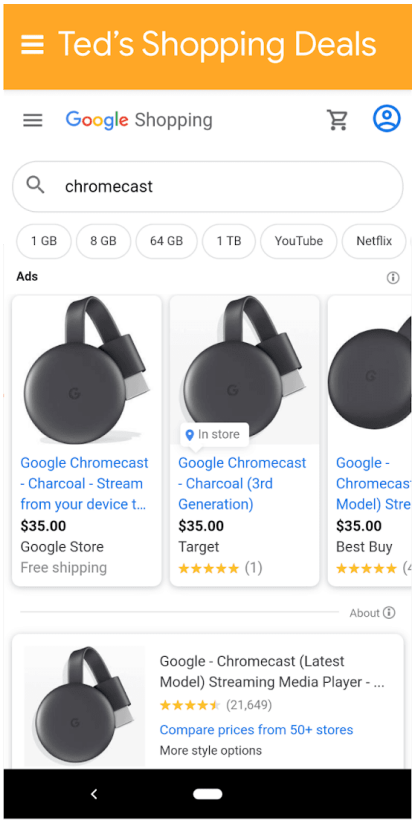
- Saat pengguna menekan tombol 'Bagikan', aplikasi langsung mengirim pesan atas nama pengguna tanpa memberi pengguna kemampuan untuk mengonfirmasi konten dan penerima yang dituju:

Spam Tampilan Web dan Afiliasi

Kami tidak mengizinkan aplikasi yang tujuan utamanya adalah mengarahkan traffic afiliasi ke sebuah situs, atau memberikan tampilan web dari situs tertentu tanpa izin pemilik atau administrator.

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.

- Aplikasi yang tujuan utamanya mengarahkan traffic rujukan ke sebuah situs untuk mendapatkan kredit pendaftaran pengguna atau pembelian di situs tersebut.
- Aplikasi yang tujuan utamanya menampilkan WebView dari situs tertentu tanpa izin:



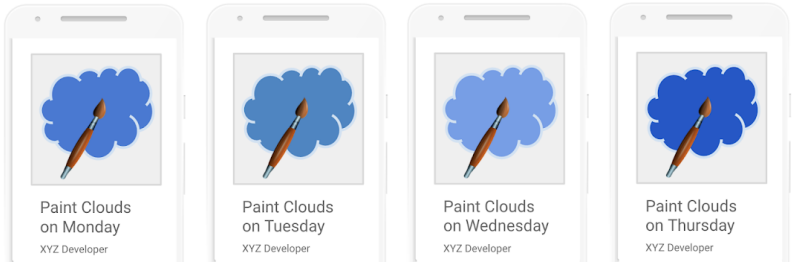
① Aplikasi ini bernama "Ted's Shopping Deals" dan hanya menampilkan WebView Google Shopping.

Konten Berulang

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

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.

- Menyalin konten dari aplikasi lain tanpa menambahkan konten atau nilai orisinal 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.



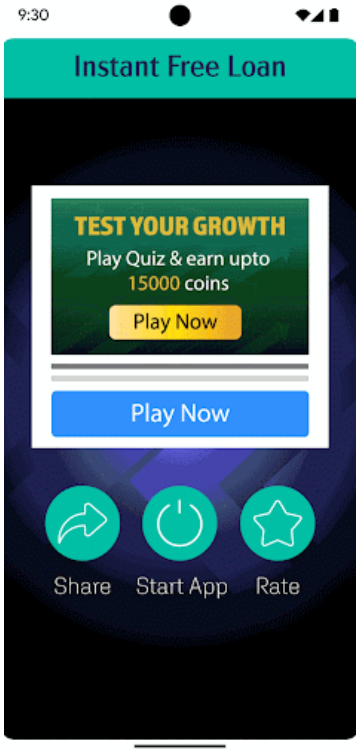
Dibuat untuk Iklan

Kami tidak mengizinkan aplikasi yang menampilkan iklan interstisial secara berulang untuk mengganggu pengguna ketika berinteraksi dengan aplikasi dan beraktivitas di dalam aplikasi.

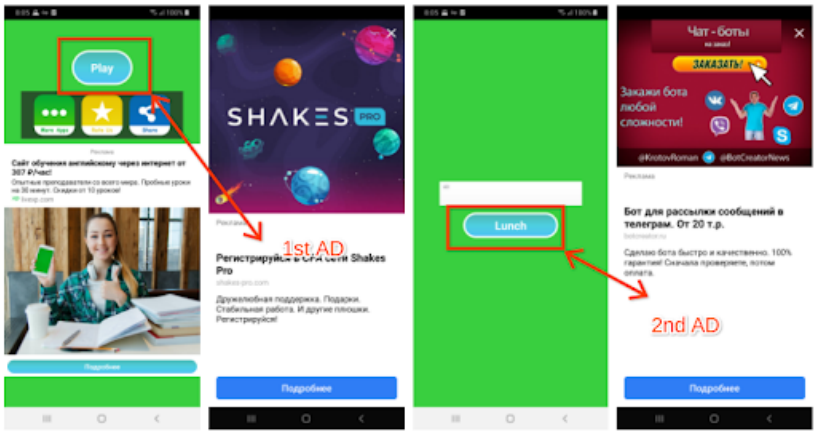
Untuk memastikan bahwa Google Play tetap menjadi platform yang aman dan sopan, kami telah membuat standar yang mendefinisikan dan melarang konten yang berbahaya atau tidak pantas bagi

pengguna kami.

- Aplikasi yang menjadi tempat munculnya iklan interstisial setelah tindakan pengguna (termasuk, tetapi tidak terbatas pada, klik, geser, dll.) secara berurutan.



Halaman pertama dalam aplikasi memiliki beberapa tombol untuk berinteraksi. Saat pengguna mengklik **Mulai aplikasi** untuk menggunakan aplikasi, muncul iklan interstisial. Setelah iklan ditutup, pengguna kembali ke aplikasi dan mengklik **Layanan** untuk mulai menggunakan layanan, tetapi muncul iklan interstisial lainnya.



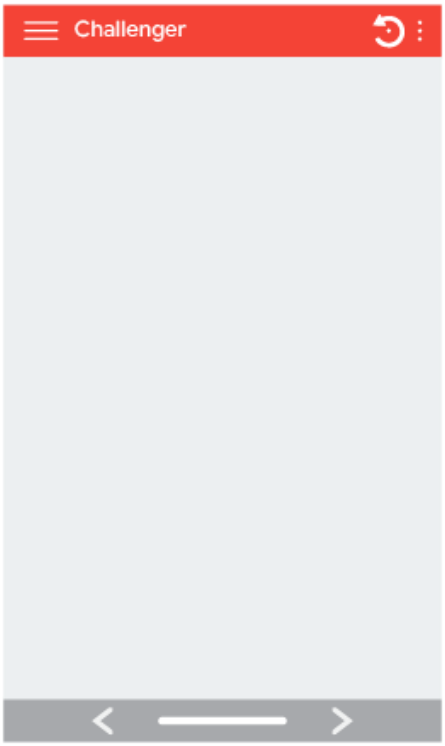
Pada halaman pertama, pengguna diarahkan untuk mengklik **Main** sebab itu merupakan satu-satunya tombol yang ada dalam aplikasi. Saat pengguna mengkliknya, muncul iklan interstisial. Setelah iklan ditutup, pengguna mengklik **Luncurkan** sebab itu merupakan satu-satunya tombol yang ada, dan muncul iklan interstisial lainnya.

Minim Fungsi

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

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.

- Aplikasi yang didesain tanpa fungsi atau tidak melakukan apa pun



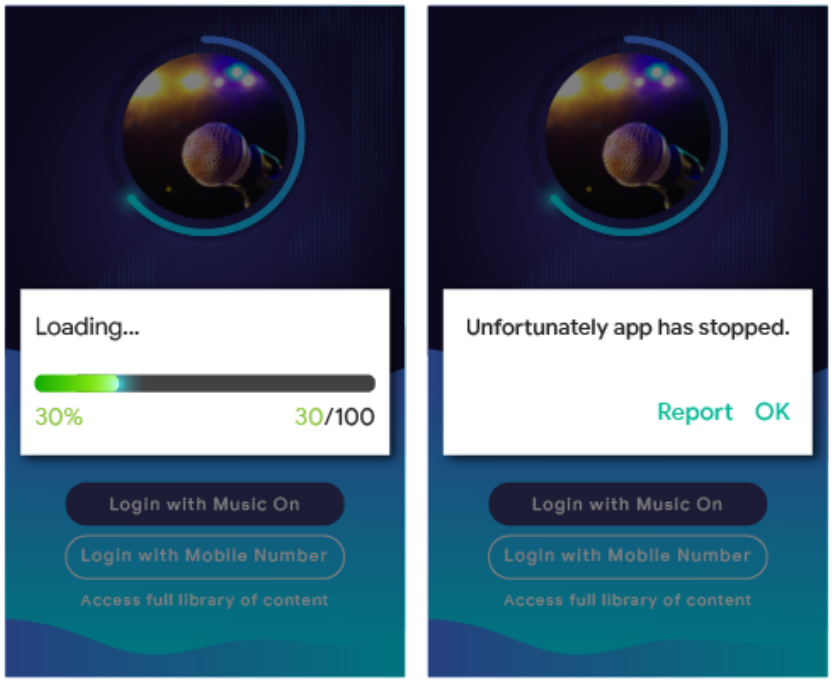
Fungsi Rusak

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

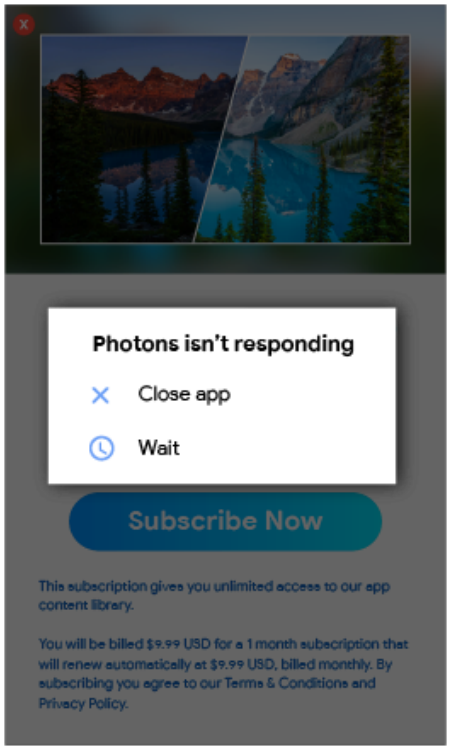
Untuk memastikan bahwa Google Play tetap menjadi platform yang aman dan sopan, kami telah membuat standar yang mendefinisikan dan melarang konten yang berbahaya atau tidak pantas bagi pengguna kami.

- Aplikasi yang **tidak dapat diinstal**

- Aplikasi yang dapat diinstal, tetapi **tidak dapat dimuat**



- Aplikasi yang dapat dimuat, 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

Tujuan kami membuat Aplikasi Instan Android adalah memberikan pengalaman pengguna yang menyenangkan dan tanpa gangguan, sekaligus mematuhi standar tertinggi privasi dan keamanan. Kebijakan kami dirancang untuk mendukung tujuan tersebut.

Developer yang memilih untuk mendistribusikan Aplikasi Instan Android melalui Google Play harus mematuhi kebijakan berikut ini, di samping semua Kebijakan Program Developer Google Play lainnya.

Identitas

Untuk aplikasi instan yang menyertakan fungsi login, developer harus mengintegrasikan Smart Lock untuk Sandi .

Dukungan Link

Developer Aplikasi Instan Android harus mendukung link untuk aplikasi lain dengan benar. Jika aplikasi instan, atau aplikasi yang diinstal milik developer, berisi link yang berpotensi tertuju ke aplikasi instan, developer harus mengirim pengguna ke aplikasi instan tersebut, bukan menangkap link di WebView , misalnya.

Spesifikasi Teknis

Developer harus mematuhi spesifikasi dan persyaratan teknis Aplikasi Instan Android yang diberikan oleh Google, yang dapat diubah dari waktu ke waktu, termasuk yang tercantum dalam dokumentasi publik kami .

Menawarkan Penginstalan Aplikasi

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

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

Pedoman UX dan detail aplikasi instan tambahan dapat ditemukan dalam Praktik Terbaik untuk Pengalaman Pengguna .

Mengubah Status Perangkat

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

Visibilitas Aplikasi

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

ID Perangkat

Aplikasi instan tidak boleh mengakses ID perangkat yang (1) tetap ada setelah aplikasi instan berhenti berjalan dan (2) tidak dapat direset oleh pengguna. Contohnya 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.

Kebijakan Emoji Android

Kebijakan emoji kami dirancang untuk mempromosikan pengalaman pengguna yang inklusif dan konsisten. Untuk mewujudkannya, semua aplikasi harus mendukung Emoji Unicode versi terbaru saat dijalankan di Android 12 atau yang lebih baru.

Aplikasi yang menggunakan Emoji Android default tanpa implementasi kustom sudah menggunakan Emoji Unicode versi terbaru saat dijalankan di Android 12 atau yang lebih baru.

Aplikasi dengan implementasi emoji kustom, termasuk yang disediakan oleh library pihak ketiga, harus sepenuhnya mendukung Unicode versi terbaru saat dijalankan di Android 12 atau yang lebih baru dalam waktu 4 bulan setelah perilisan Emoji Unicode baru.

Baca panduan ini untuk mempelajari cara mendukung emoji modern.

Gunakan contoh emoji di bawah ini untuk menguji apakah aplikasi Anda sesuai dengan Versi Unicode terbaru:

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

Keluarga

Google Play menawarkan platform kaya bagi developer untuk menampilkan konten mereka yang berkualitas tinggi dan sesuai untuk usia seluruh anggota keluarga. 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 undang-undang 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 memperkaya kehidupan keluarga terus berkembang, dan para orang tua kini mencari konten 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. Andalah 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 dewasa, 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 dalam Program Disetujui Pengajar, tetapi kami tidak dapat menjamin bahwa aplikasi Anda akan diikutsertakan dalam Program Disetujui 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

Di bagian Target Audiens dan Konten di Konsol Google Play, Anda harus menunjukkan target audiens untuk aplikasi Anda sebelum memublikasikannya, dengan memilih opsi dari daftar kelompok usia yang disediakan. Terlepas dari opsi yang Anda tentukan di Konsol Google Play, jika Anda memilih untuk menyertakan citra atau istilah dalam aplikasi yang dapat dianggap menargetkan anak-anak, 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.

Pilihlah lebih dari satu kelompok usia untuk target audiens aplikasi hanya 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 dirancang 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.

Pembaruan untuk 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 harus dilakukan sebelum informasi ini ditampilkan di Google Play Store. Namun, perubahan apa pun yang Anda lakukan pada bagian ini di Konsol Google Play mungkin akan ditinjau terkait kepatuhan 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 atas segala informasi tentang aplikasi Anda di Konsol Google Play, termasuk di bagian Target Audiens dan Konten, dapat berakibat pada penghapusan atau penangguhan aplikasi sehingga Anda harus menyediakan informasi yang akurat.

Persyaratan Kebijakan Keluarga

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

1. **Konten aplikasi:** Konten aplikasi Anda yang dapat diakses oleh anak-anak harus sesuai untuk anak-anak. Jika aplikasi Anda berisi konten yang tidak sesuai secara global, tetapi konten tersebut dianggap sesuai untuk pengguna anak di wilayah tertentu, aplikasi tersedia di wilayah tersebut (wilayah terbatas), tetapi tidak tersedia di wilayah lain.
2. **Fungsi aplikasi:** Aplikasi Anda tidak boleh hanya menyediakan WebView dari suatu situs atau memiliki tujuan utama untuk mendorong traffic afiliasi ke suatu situs, terlepas dari status kepemilikan situs tersebut.
   - Kami terus berupaya mencari berbagai cara untuk memberikan pengalaman baru bagi developer aplikasi anak-anak. Jika Anda berminat mengikuti uji coba Aplikasi Web Tepercaya kami untuk aplikasi edukasi, harap beri tahukan minat Anda di sini .
3. **Jawaban Konsol Play:** Anda harus menjawab pertanyaan mengenai aplikasi Anda dengan tepat di Konsol Play, dan memperbarui jawaban tersebut untuk merefleksikan setiap perubahan pada aplikasi Anda secara akurat. Hal ini termasuk, tetapi tidak terbatas pada, mengungkapkan elemen interaktif aplikasi Anda secara akurat pada Kuesioner Rating Konten, seperti:
   - Pengguna aplikasi Anda dapat berinteraksi atau bertukar informasi;
   - Aplikasi Anda membagikan informasi yang diberikan pengguna kepada pihak ketiga; dan
   - Aplikasi Anda membagikan lokasi fisik pengguna kepada pengguna lain.
4. **Iklan:** Jika aplikasi Anda menampilkan iklan kepada anak-anak atau kepada pengguna dengan usia yang tidak diketahui, Anda harus:
   - Hanya menggunakan SDK iklan tersertifikasi Google Play 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.
5. **Praktik 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, dan data penggunaan iklan. Anda juga harus memastikan bahwa aplikasi mengikuti praktik data di bawah:
   - Aplikasi yang hanya menargetkan anak-anak tidak boleh mentransmisikan ID iklan Android (AAID), Nomor Seri SIM, Nomor Seri Build, BSSID, MAC, SSID, IMEI, dan/atau IMSI.
   - Aplikasi yang menargetkan audiens anak-anak dan dewasa tidak boleh mentransmisikan AAID, Nomor Seri SIM, Nomor Seri Build, BSSID, MAC, SSID, IMEI, dan/atau IMSI dari anak-anak atau pengguna yang tidak diketahui usianya.
   - Nomor telepon perangkat tidak boleh diminta dari TelephonyManager di Android API.
   - Aplikasi yang hanya menargetkan anak-anak tidak boleh meminta izin lokasi, atau mengumpulkan, menggunakan, dan mengirimkan lokasi akurat .
   - Aplikasi harus menggunakan Companion Device Manager (CDM) saat meminta akses Bluetooth, kecuali aplikasi Anda hanya menargetkan versi Sistem Operasi (OS) perangkat yang

tidak kompatibel dengan CDM.

6. **API dan SDK:** Anda harus memastikan bahwa aplikasi Anda mengimplementasikan setiap API dan SDK dengan benar.
   - Aplikasi yang hanya menargetkan anak-anak tidak boleh memuat API atau SDK yang tidak disetujui untuk digunakan dalam layanan yang terutama ditujukan untuk anak-anak. Hal 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 dewasa tidak boleh mengimplementasikan API atau SDK yang tidak disetujui penggunaannya dalam layanan yang ditujukan untuk anak-anak, kecuali jika digunakan di balik layar verifikasi usia atau diimplementasikan tanpa mengumpulkan data dari anak-anak. Aplikasi yang menargetkan audiens anak-anak dan dewasa 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.
7. **Augmented Reality (AR):** Jika aplikasi Anda menggunakan Augmented Reality, Anda harus menyertakan peringatan keamanan langsung setelah bagian AR diluncurkan. Peringatan harus memuat hal berikut:
   - Pesan yang sesuai tentang pentingnya pengawasan orang tua.
   - Pengingat untuk mewaspadai 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. **Fitur & Aplikasi Sosial:** Jika aplikasi Anda mengizinkan pengguna untuk berbagi atau bertukar informasi, Anda harus mengungkapkan fitur ini secara akurat dalam kuesioner rating konten di Konsol Play.
   - Aplikasi Sosial: Aplikasi sosial adalah aplikasi yang fokus utamanya adalah memungkinkan pengguna berbagi konten berformat bebas atau berkomunikasi dengan banyak orang. Semua aplikasi sosial yang menyertakan anak-anak dalam target audiensnya harus menyediakan pengingat dalam aplikasi agar aman saat online dan menyadari risiko dunia nyata dari interaksi online sebelum mengizinkan pengguna anak untuk bertukar media atau informasi berformat bebas. Anda juga harus meminta tindakan orang dewasa sebelum mengizinkan pengguna anak untuk bertukar informasi pribadi.
   - Fitur Sosial: Fitur sosial adalah fungsi aplikasi tambahan apa pun yang memungkinkan pengguna berbagi konten berformat bebas atau berkomunikasi dengan banyak orang. Aplikasi apa pun yang menyertakan anak-anak dalam target audiensnya dan memiliki fitur sosial, harus menyediakan pengingat dalam aplikasi agar aman saat online dan menyadari risiko dunia nyata dari interaksi online sebelum mengizinkan pengguna anak bertukar media atau informasi berformat bebas. Anda juga harus menyediakan metode bagi orang dewasa untuk mengelola fitur sosial bagi pengguna anak, termasuk, tetapi tidak terbatas pada, mengaktifkan/menonaktifkan fitur sosial atau memilih tingkat fungsi yang berbeda. Terakhir, Anda harus meminta tindakan orang dewasa sebelum mengaktifkan fitur yang memungkinkan anak-anak bertukar informasi pribadi.
   - Tindakan orang dewasa berarti mekanisme untuk memverifikasi bahwa pengguna tersebut bukan anak-anak dan tidak mendorong anak-anak untuk memalsukan usia mereka demi mendapatkan akses ke area aplikasi Anda yang didesain untuk orang dewasa (yaitu PIN orang dewasa, sandi, tanggal lahir, verifikasi email, ID foto, kartu kredit, atau SSN).
   - Aplikasi sosial yang fokus utamanya adalah untuk melakukan chat dengan orang yang tidak mereka kenal tidak boleh menargetkan anak-anak. Contohnya termasuk: aplikasi gaya roulette chat, aplikasi kencan, ruang chat terbuka yang berfokus pada anak-anak, dll.
9. **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 lainnya yang berlaku.

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.

- Aplikasi yang mempromosikan permainan untuk anak-anak di listingan Play Store, tetapi konten dari aplikasi tersebut 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. Harap baca kebijakan Iklan Keluarga dan Monetisasi untuk mengetahui informasi lebih lanjut 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 (aplikasi harus diberi rating sebagai ESRB Everyone atau Everyone 10+, atau yang setara) dan hanya boleh menggunakan SDK iklan tersertifikasi Google Play . 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.

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

- 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

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 dan membuat 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

Jika Anda memonetisasi aplikasi yang menargetkan anak-anak di Play, aplikasi Anda harus mengikuti Persyaratan Kebijakan Monetisasi dan Iklan Keluarga berikut.

Kebijakan di bawah berlaku untuk semua monetisasi dan iklan di aplikasi Anda, termasuk iklan, promosi silang (untuk aplikasi Anda dan aplikasi pihak ketiga Anda), penawaran untuk pembelian dalam aplikasi, atau konten komersial lainnya (seperti penempatan produk berbayar). Semua monetisasi dan iklan 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

Monetisasi dan iklan di aplikasi Anda tidak boleh memiliki konten yang menipu atau dirancang sedemikian rupa sehingga akan menghasilkan klik yang tidak disengaja dari pengguna anak. Berikut adalah hal-hal yang dilarang:

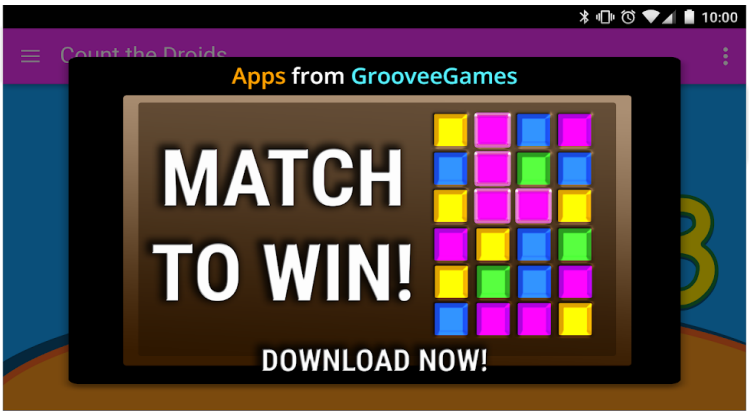
- Monetisasi dan iklan yang mengganggu, termasuk monetisasi dan iklan yang memenuhi seluruh layar atau mengganggu penggunaan normal dan tidak memberikan cara yang jelas untuk menutup iklan (misalnya Dinding iklan)
- Monetisasi dan iklan yang mengganggu penggunaan normal aplikasi atau alur game, yang tidak dapat ditutup setelah 5 detik.
- Monetisasi dan iklan yang tidak mengganggu penggunaan normal aplikasi atau alur game boleh ditayangkan selama lebih dari 5 detik (misalnya konten video dengan iklan terintegrasi).
- Monetisasi dan iklan interstisial 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).
- Monetisasi dan iklan 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

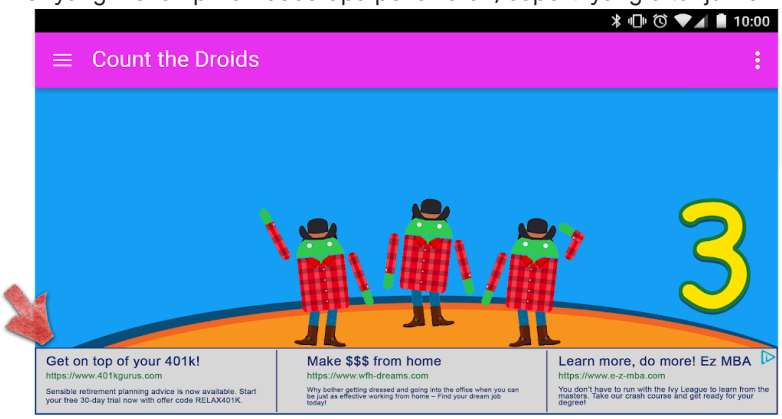
Untuk memastikan bahwa Google Play tetap menjadi platform yang aman dan sopan, kami telah membuat standar yang mendefinisikan dan melarang konten yang berbahaya atau tidak pantas bagi pengguna kami.

- Monetisasi dan iklan yang menjauh dari jari pengguna saat pengguna mencoba menutup iklan
- Monetisasi dan iklan yang memungkinkan pengguna keluar dari penawaran setelah lima (5) detik sebagaimana ditunjukkan dalam contoh di bawah:

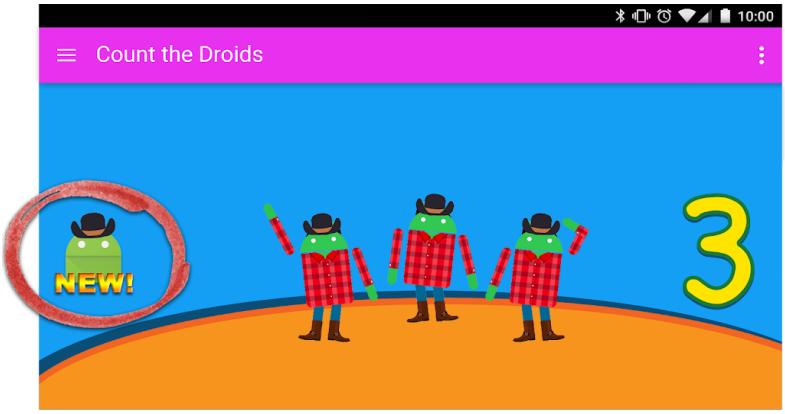
- Monetisasi dan iklan yang menggunakan sebagian besar ruang di layar perangkat tanpa memberikan cara yang jelas kepada pengguna untuk menutupnya, sebagaimana ditunjukkan dalam contoh di bawah:



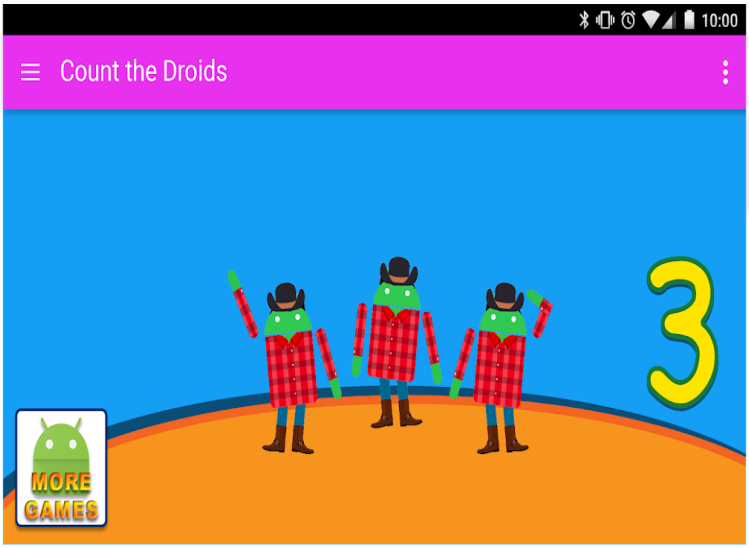
- Iklan banner yang menampilkan beberapa penawaran, seperti yang ditunjukkan dalam contoh di bawah:



- Monetisasi dan iklan yang dapat disalahartikan oleh pengguna sebagai konten aplikasi, seperti yang ditunjukkan dalam contoh di bawah:



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



Berikut beberapa contoh konten iklan yang tidak pantas dan 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 gratis untuk mengikutinya.
- **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 berisi konten kekerasan yang tidak sesuai untuk anak-anak.

SDK Iklan

Jika Anda menayangkan iklan dalam aplikasi dan satu-satunya target audiens Anda adalah anak-anak, Anda hanya boleh menggunakan SDK iklan tersertifikasi mandiri Keluarga . 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 mandiri Keluarga. Aplikasi dalam program Didesain untuk Keluarga diwajibkan untuk hanya menggunakan SDK iklan tesertifikasi mandiri.

Harap buka halaman kebijakan Program SDK Iklan Tesertifikasi Mandiri Keluarga untuk detail selengkapnya mengenai persyaratan ini dan untuk melihat daftar terbaru SDK iklan tersertifikasi mandiri.

Jika Anda menggunakan AdMob, lihat Pusat Bantuan AdMob untuk mengetahui 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.

Pembelian dalam aplikasi

Google Play akan mengautentikasi ulang semua pengguna sebelum melakukan pembelian dalam aplikasi pada aplikasi yang berpartisipasi dalam program Didesain untuk Keluarga. Langkah ini bertujuan untuk 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 itu benar-benar terjadi, kami berkomitmen untuk memastikan bahwa developer mengetahui cara agar aplikasinya tetap patuh pada peraturan yang ada. Harap beri tahu kami jika Anda melihat pelanggaran atau memiliki pertanyaan tentang mengelola pelanggaran .

Cakupan Kebijakan

Kebijakan kami berlaku untuk konten apa pun yang ditampilkan atau ditautkan oleh aplikasi Anda, termasuk iklan apa pun yang ditampilkan ke pengguna, dan konten buatan pengguna apa pun 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 penginstalan, 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.

Persyaratan yang dijelaskan dan digunakan dalam kebijakan ini memiliki maksud yang sama dengan yang ada dalam Perjanjian Distribusi Developer (DDA). Selain mematuhi kebijakan ini dan DDA, konten aplikasi Anda harus diberi rating sesuai dengan Pedoman Rating Konten kami.

Kami tidak mengizinkan aplikasi atau konten aplikasi yang merusak kepercayaan pengguna dalam ekosistem Google Play. 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 mengidentifikasi risiko penyalahgunaan termasuk, tetapi tidak terbatas pada, hal-hal seperti keluhan khusus aplikasi dan developer, pelaporan berita, histori pelanggaran sebelumnya, masukan pengguna, dan penggunaan merek, 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 penginstalannya 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 .

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 melihat lagi listingan Play Store, jumlah instal pengguna yang sudah ada, statistik, dan rating untuk aplikasi tersebut. Informasi ini akan dipulihkan setelah Anda mengirim update yang mematuhi kebijakan.

- Anda tidak dapat menggunakan lagi 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 Anda 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.

Wilayah Terbatas

- Aplikasi Anda hanya dapat didownload oleh pengguna melalui Google Play di wilayah tertentu.
- Pengguna dari wilayah lain tidak akan dapat menemukan aplikasi tersebut di Play Store.
- Pengguna yang sebelumnya menginstal aplikasi tersebut dapat terus menggunakannya di perangkat mereka, tetapi tidak akan menerima update lagi.
- Pembatasan wilayah tidak memengaruhi status akun Developer Google Play Anda.

Penghentian Akun

- Jika akun developer Anda dihentikan, semua aplikasi dalam katalog Anda akan dihapus dari Google Play dan Anda tidak dapat memublikasikan aplikasi baru lagi. 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.

Akun Dorman

Akun dorman adalah akun developer yang tidak aktif atau diabaikan. Akun dorman tidak memiliki reputasi baik seperti yang diwajibkan oleh Perjanjian Distribusi Developer .

Akun Developer Google Play ditujukan untuk developer aktif yang memublikasikan dan memelihara aplikasi secara aktif. Untuk mencegah penyalahgunaan, kami menutup akun dorman atau yang tidak digunakan atau tidak sering terlibat (misalnya untuk memublikasikan dan mengupdate aplikasi, mengakses statistik, atau mengelola listingan Play Store) secara berkala.

Penutupan akun dorman akan menghapus akun Anda dan semua data yang terkait dengan akun tersebut. Biaya pendaftaran Anda tidak dapat dikembalikan dan akan hangus. Sebelum kami menutup akun dorman Anda, kami akan memberi tahu Anda menggunakan informasi kontak yang Anda berikan untuk akun tersebut.

Penutupan akun dorman tidak akan membatasi kemampuan Anda untuk membuat akun baru di masa mendatang jika Anda memutuskan untuk memublikasikannya di Google Play. Anda tidak akan dapat mengaktifkan kembali akun Anda dan aplikasi atau data apa pun sebelumnya tidak akan tersedia di akun baru.

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 aplikasi
- Melaporkan pelanggaran kebijakan
- Hubungi Google Play tentang 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

Persyaratan Konsol Play

Google Play ingin memberikan pengalaman aplikasi yang aman dan luar biasa bagi pengguna kami serta peluang besar bagi semua developer kami agar sukses. Kami berusaha untuk memastikan bahwa proses penyediaan aplikasi Anda untuk pengguna berjalan selancar mungkin.

Untuk membantu Anda menghindari pelanggaran umum yang dapat memperlambat proses peninjauan atau memicu penolakan, pastikan Anda melakukan hal berikut saat mengirimkan informasi melalui Konsol Play.

Sebelum mengirimkan aplikasi, Anda harus:

- Memberikan semua informasi dan metadata aplikasi secara akurat
- Memastikan bahwa informasi kontak Anda sudah diperbarui
- Mengupload kebijakan privasi aplikasi Anda dan melengkapi persyaratan bagian **Keamanan Data**
- Memberikan akun demo aktif, informasi login, dan semua referensi yang diperlukan untuk meninjau aplikasi Anda (yaitu, kredensial login, kode QR, dll.)

Seperti biasa, Anda harus memastikan bahwa aplikasi Anda memberikan pengalaman pengguna yang stabil, menarik, dan responsif; pastikan bahwa segala yang ada di aplikasi Anda, termasuk jaringan iklan, layanan analisis, dan SDK pihak ketiga, mematuhi Kebijakan Program Developer Google Play; dan jika target audiens aplikasi Anda adalah anak-anak, pastikan Anda mematuhi Kebijakan keluarga kami.

Perlu diingat, Anda bertanggung jawab untuk membaca Perjanjian Distribusi Developer dan semua Kebijakan Program Developer guna memastikan bahwa aplikasi Anda patuh sepenuhnya.

Developer Distribution Agreement

Perlu bantuan lain?

Coba langkah-langkah selanjutnya berikut:

Hubungi kami

Beri tahu kami selengkapnya dan kami akan membantu Anda