

Geliştirici Program Politikası (1 Mart 2021'den itibaren geçerlidir)

Gelin hep birlikte, uygulamalar ve oyunlar için dünyanın en güvenilir kaynağını oluşturalım

Sunduğunuz yenilikler, tüm geliştiricilerle paylaştığımız başarının temelini oluşturur, ancak bu başarı beraberinde sorumluluk da getirir. Geliştirici Program Politikaları ve [Geliştirici Dağıtım Sözleşmesi](#), birlikte dünyanın en yenilikçi ve güvenilir uygulamalarını Google Play üzerinden bir milyarı aşkın kullanıcıya sunmaya devam etmemizi sağlar. Sizi aşağıdaki politikalarımızı keşfetmeye davet ediyoruz.

Kısıtlanmış İçerik

Dünyanın her yerinden kullanıcılar, Google Play'i kullanarak her gün uygulama ve oyunlara erişiyor. Bir uygulamayı göndermeden önce, kendinize uygulamanızın Google Play için uygun olup olmadığını, yerel yasalara uyup uymadığını sorun.

Çocukların Tehlikeye Atılması

Küçüklerin cinsel açıdan tasvir edildiği içerikler barındıran uygulamalar, Google Store'dan hemen kaldırılır.-Pedofiliyi veya reşit olmayan kişilerle uygunsuz etkileşimleri (ör. elle taciz veya okşama) destekleyen uygulamalar da buna dahildir, ancak maddenin kapsamı bunlarla sınırlı değildir.

Ayrıca, aşırı şiddet ve kan içeren ya da zararlı ve tehlikeli etkinlikleri tasvir veya teşvik eden uygulamalar da dahil ancak bunlarla sınırlı olmamak üzere, çocuklara hitap etmesine rağmen yetişkinlere uygun temalar barındıran uygulamalara izin verilmez. Estetik cerrahi veya kilo verme gibi kişinin fiziksel görünümünde yapılan kozmetik değişiklikleri eğlence malzemesi yaparak tasvir eden uygulamalar da dahil olmak üzere kişinin bedeniyle veya kendiyile ilgili olumsuz bir algıya sahip olmasına yol açabilecek uygulamalara da izin verilmez.

Bir ögenin içinde çocukların bulunduğu cinsel içerik barındırdığını belirlersek durumu yetkililere bildirir ve içeriğin dağıtımında yer alan kişilerin Google Hesaplarını sileriz.

Uygunsuz İçerik

Google Play'in güvenli ve saygılı bir platform olarak kalmasını sağlamak amacıyla, kullanıcılarımız için zararlı ya da uygunsuz olan içerikleri tanımlayan ve yasaklayan standartlar oluşturduk.

Cinsel İçerik ve Küfür

Pornografi veya cinsel açıdan tatmin edici olması amaçlanan içerik ya da hizmetler dahil olmak üzere cinsel içerik veya küfür barındıran ya da bunların tanıtımını yapan uygulamalara izin verilmez. Çıplaklık barındıran içeriklere, birincil amacı eğitim, belgesel, bilimsel veya sanatsal olup cinsel tatmine yönelik olmadıkları takdirde izin verilebilir.

Yaygın görülen ihlallere ilişkin bazı örnekleri aşağıda bulabilirsiniz:

- Öznenin çıplak, bulanıklaştırılmış veya minimum düzeyde giyinik olduğu ve/veya giysisinin herkese açık bağlamda uygun kabul edilmeyeceği bir durumda tasvir edilen cinsel içerikli çıplaklık ya da müstehcen pozlar.
- Cinsel ilişki veya müstehcen pozların tasviri, animasyonu veya çizimleri ya da organların cinsel açıdan tasviri.
- Cinsel amaçlı kullanılan aletlerin, cinsellik rehberlerinin, yasa dışı cinsellik temalarının ve fetiş nesnelerinin tasvirlerini barındıran veya bu işleve sahip içerikler.
- Açık saçık veya küfür barındıran içerikler (mağaza girişi veya uygulama içinde küfür, hakaret, müstehcen metin, yetişkinlere uygun/cinsellikle ilgili anahtar kelimeler barındıran içerikler de dahil ancak bunlarla sınırlı olmamak üzere).
- Hayvanlarla cinsel ilişkiyi tasvir eden, açıklayan veya teşvik eden içerik.
- Cinsellikle ilgili eğlence, eskort hizmetleri veya ücret karşılığında cinsel eylemler sağlıyormuş gibi yorumlanabilecek diğer hizmetleri tanıtan uygulamalar.
- Kişileri aşağılayan veya nesneleştiren uygulamalar.

Nefret Söylemi

Şiddeti özendiren veya ırk, etnik köken, din, engellilik, yaş, uyruk, gazilik durumu, cinsel yönelim, cinsiyet, cinsel kimlik veya sistematik ayrımcılık ya da ötekileştirmeye ilişkin ilişkili diğer özelliklere göre bireylere veya gruplara karşı nefreti teşvik eden uygulamalara izin verilmez.

Bazı ülkelerde yerel yasa ve yönetmeliklere göre, Nazilerle ilgili EBBS (Eğitimsel, Belgesel, Bilimsel veya Sanatsal) içerik barındıran uygulamalar engellenebilir.

Yaygın görülen ihlallere dair örnekleri aşağıda bulabilirsiniz:

- Koruma altındaki bir grubun insan olmadığını, değersiz veya nefrete layık olduğunu iddia eden içerik veya konuşma.
- Koruma altındaki bir grubun olumsuz özellikleri (ör. kötü amaçlı, yozlaşmış, uğursuz olduğu vb.) ile ilgili teoriler, nefret dolu hakaretler veya klişeler içeren ya da grubun açıkça veya ima yoluyla tehdit oluşturduğunu iddia eden uygulamalar.
- Koruma altındaki bir grubun üyesi olan kişilerden nefret edilmesi veya bu tür kişilere ayrımcılık yapılması gerektiği yönünde diğer kişileri teşvik etmeye çalışan içerik veya konuşma.
- Nefret edilen gruplarla ilişkilendirilen bayrak, sembol, işaret, eşya gibi nefret sembollerini veya davranışları destekleyip bunların tanıtımını yapan içerikler.

Şiddet

Nedensiz şiddet veya diğer tehlikeli etkinlikleri tasvir eden ya da kolaylaştıran uygulamalara izin verilmez. Kurgusal şiddeti oyun bağlamında (ör. çizgi film, avlanma veya balık tutma) tasvir eden uygulamalara genellikle izin verilir.

Yaygın görülen ihlallere ilişkin bazı örnekleri aşağıda bulabilirsiniz:

- Herhangi bir kişiye veya hayvana yönelik gerçekçi şiddet ya da şiddet içeren tehditlerin grafik tasvirleri veya açıklamaları.
- Kendine zarar verme, intihar, zorbalık, taciz, yeme bozuklukları, boğulma oyunları veya ciddi yaralanma ya da ölümle sonuçlanabilecek diğer eylemleri teşvik eden uygulamalar.

Terör Amaçlı İçerik

Terör örgütlerinin, adam toplamak da dahil, herhangi bir amaçla Google Play'de uygulama yayınlamasına izin verilmez.

Terörizmle alakalı içerik (terörist faaliyetleri destekleyen, şiddeti teşvik eden veya terör saldırılarını öven içerikler gibi) barındıran uygulamalara izin verilmez. Terörizm ile ilgili içerikler yayınlamanızın nedeni eğitici, belge niteliği taşıyan, bilimsel veya sanatsal bir paylaşım yapmaksa kullanıcıların bağlamı doğru bir şekilde anlamalarına yardımcı olacak düzeyde bilgi sağlamaya çalışın.

Hassas Olaylar

Doğal afet, zulüm, savaş, ölüm veya başka bir trajik olaya karşı makul hassasiyeti göstermeyen ya da böyle bir olayı istismar eden uygulamalara izin verilmez. Hassas bir olayla alakalı içerik barındıran uygulamalara genellikle söz konusu içerik EBBS (Eğitimsel, Belgesel, Bilimsel veya Sanatsal) değeri taşıyorsa ya da kullanıcıları hassas olaya karşı uyarmayı veya onlara farkındalık kazandırmayı amaçlıyorsa izin verilir.

Yaygın görülen ihlallere dair örnekleri aşağıda bulabilirsiniz:

- Gerçek kişi veya kişilerin intihar, aşırı dozda uyuşturucu kullanımı, doğal nedenler gibi sebeplere bağlı olarak ölmelerine hassasiyet göstermeme.
- Önemli bir trajik olayı inkar etme.
- Trajik bir olaydan, olayın kurbanlarının açıkça yararına olmayan bir şekilde kazanç elde ediyor görünme.

Zorbalık ve Taciz

Tehdit, taciz veya zorbalık içeren veya bunları kolaylaştıran uygulamalara izin verilmez.

Yaygın görülen ihlallere dair örnekleri aşağıda bulabilirsiniz:

- Uluslararası veya dinsel çatışmaların kurbanlarına zorbalık yapma.
- Başka kişileri gasp etme, şantaj yapma gibi yöntemler de dahil olmak üzere çeşitli şekillerde sömürmeye çalışan içerik.
- Başkasını herkese açık bir şekilde aşağılamak amacıyla içerik yayınlama.
- Trajik bir olayın kurbanlarına veya arkadaşlarına ve ailelerine zorbalık yapma.

Tehlikeli Ürünler

Patlayıcı madde, ateşli silah, mühimmat veya belirli ateşli silah aksesuarı satışına hizmet eden uygulamalara izin verilmez.

- Kısıtlanan aksesuarlara, ateşli bir silahın otomatik silah gibi davranmasını sağlamayı veya ateşli bir silahı otomatik silaha dönüştürmeyi (ör. yatay hareketli dipçik, mitralyöz tetik, dönüştürme seti) sağlayan aksesuarlar ve 30 atımdan

daha fazla şarjör veya kayış taşıyan aksesuarlar dahildir.

Patlayıcı, ateşli silah, mühimmat, kısıtlı ateşli silah veya diğer silahları üretmek için talimat sağlayan uygulamalara izin verilmez. Buna bir ateşli silahı otomatik silaha veya otomatik gibi çalışan ateşli silaha dönüştürme talimatları da dahildir.

Marihuana

Yasal olup olmamasından bağımsız olarak marihuana veya marihuana ürünlerinin satışını sağlayan uygulamalara izin verilmez.

Yaygın görülen ihlallere ilişkin bazı örnekleri aşağıda bulabilirsiniz:

- Uygulama içi alışveriş sepeti özelliği ile kullanıcıların marihuana siparişi vermelerine olanak sağlama.
- Kullanıcıların adreslerine marihuana gönderilmesine veya yerinden almalarına yardımcı olma.
- THC (tetrahidrokanabinol) içeren kanabidiol (CBD) yağları gibi ürünler de dahil olmak üzere THC içeren ürünlerin satışını kolaylaştırma.

Tütün ve Alkol

E-sigaralar da dahil olmak üzere tütün satışını kolaylaştıran veya alkol ya da tütünün yasa dışı veya uygunsuz kullanımını teşvik eden uygulamalara izin verilmez.

Yaygın görülen ihlallere dair örnekleri aşağıda bulabilirsiniz:

- Küçüklere alkol veya tütün kullanımı ya da satışını anlatma veya teşvik etme.
- Tütün tüketiminin sosyal, cinsel, mesleki, entelektüel veya sportif gücü artırabileceğini ima etme.
- Aşırı veya uzun süreli içki tüketimi ya da içki yarışmalarının olumlu gösterilmesi de dahil olmak üzere aşırı içki tüketiminin tanıtımını yapma.

Mali Hizmetler

Kullanıcıları yanıltıcı veya zararlı finansal ürünler ve hizmetlere maruz bırakan uygulamalara izin verilmez.

Bu politikanın amacı doğrultusunda, para ve kripto para birimlerinin yönetimi veya yatırımıyla ilgili ürün ve hizmetler (kişiye özel tavsiyeler dahil) finansal ürün ve hizmet olarak değerlendirilir.

Uygulamanız finansal ürünler ve hizmetler içeriyorsa veya bunların tanıtımını yapıyorsa uygulamanızın hedeflediği tüm bölge veya ülkelere ait devlet ve yerel yönetim yasalarına (ör. yerel yasaların gerektirdiği özel ifşaları içermeye) uymanız gereklidir.

İkili Opsiyonlar

Kullanıcılara ikili seçenek ticareti yapma olanağı sağlayan uygulamalara izin verilmez.

Kripto Para Birimi

Cihazlarda kripto para birimi madenciliği yapan uygulamalara izin verilmez. Kripto para birimi madenciliğini uzaktan yöneten uygulamalara izin verilir.

Bireysel krediler

Bireysel krediler bir özel kişi, kuruluş veya tüzel kişi tarafından bireysel tüketicilere bir kereliğine ve bir sabit kıymetin ya da eğitimin alınmasını finanse etme amacı dışında verilen borç para olarak tanımlanır. Bireysel kredi tüketicilerinin kredi alıp almama konusunda bilinçli kararlar verebilmeleri için kredi ürünlerinin kalitesi, özellikleri, ücretleri, geri ödeme takvimi, riskleri ve avantajları hakkında bilgi sahibi olmaları gerekir.

- Örnekler: Bireysel krediler, maaş günü kredileri, eşler arası krediler, ipotekli krediler
- Dahil olmayanlar: Konut finansmanı kredileri, taşıt kredileri, öğrenim kredileri, yenilenebilen krediler (ör. kredi kartları, bireysel limitli krediler)

Doğrudan kredi sunan uygulamalar, olası satış yaratan uygulamalar ve tüketicileri üçüncü taraf kredi sağlayıcılarla iletişime geçiren uygulamalar da dahil ancak bunlarla sınırlı olmamak üzere bireysel kredi veren uygulamalar, uygulama meta verilerinde aşağıdaki bilgileri paylaşmalıdır:

- Minimum ve maksimum geri ödeme süresi.
- Genellikle bir yıllık faiz oranı, masraflar ve diğer masrafların toplanmasından oluşan Maksimum Yıllık Yüzde Oranı (APR) veya yerel yasalar çerçevesinde hesaplanmış benzer başka bir oran
- Geçerli tüm ücretler dahil olmak üzere kredinin toplam maliyetinin temsili örneği

- Kişisel ve hassas kullanıcı verilerine erişim, bu verileri toplama, kullanma ve paylaşma faaliyetlerini kapsamlı bir şekilde açıklayan bir gizlilik politikası.

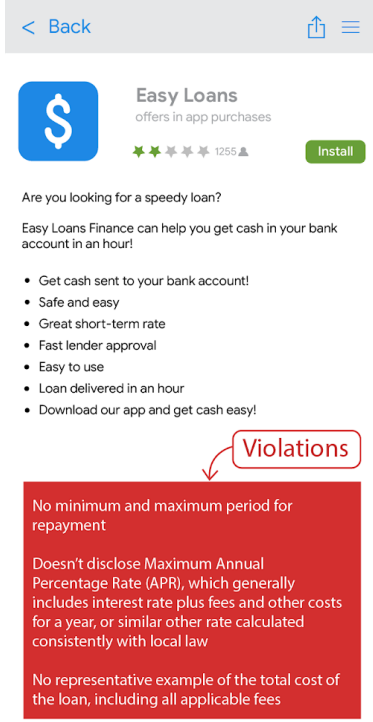
Kredinin verildiği tarihten itibaren 60 gün veya daha az süre içinde tamamen geri ödeme gerektiren bireysel kredilerin (bunlara "kısa vadeli bireysel krediler" diyoruz) tanıtımını yapan uygulamalara izin verilmez.

Yıllık Yüzde Oranı yüksek bireysel krediler

ABD'de Yıllık Yüzde Oranı (APR) %36 veya daha yüksek bireysel kredi uygulamalarına izin verilmez. ABD'deki bireysel kredi uygulamaları, [Kredilerde Doğru Bilgilendirme Yasası \(TILA\)](#) uyarınca hesaplanmış maksimum Yıllık Yüzde Oranlarını sergilemelidir.

Bu politika; doğrudan kredi sunan uygulamalar, olası satış yaratan uygulamalar ve tüketicileri üçüncü taraf kredi sağlayıcılarla iletişime geçiren uygulamalar için geçerlidir.

Sık görülen ihlallerle ilgili bir örneği aşağıda bulabilirsiniz:



Gerçek Parayla Kumar Oynama, Oyunlar ve Yarışmalar

Gerçek parayla kumar oynanan uygulamalara, gerçek parayla kumar oynamayla ilgili reklamlara ve belirli gereksinimleri karşılayan günlük fantezi spor uygulamalarına izin verilir.

Kumar Uygulamaları

Kısıtlamalara ve tüm Google Play politikalarına uymaya tabi olmak şartıyla, aşağıdaki tabloda yer alan ülkelerde çevrimiçi kumar oynama olanağı sunan veya bunu kolaylaştıran uygulamalara şu koşullar yerine getirildiği sürece izin verilir: Geliştirici, Play'de dağıtılan kumar uygulamaları için [başvuru işlemini tamamlamalıdır](#), onaylanmış bir resmi işletmeci ve/veya belirtilen ülkede ilgili resmi kumar ve talih oyunları kurumunda lisanslı bir işletmeci olarak kayıtlı olmalıdır ve sunmak istediği çevrimiçi kumar ürünü için belirtilen ülkede geçerli bir işletme lisansı sunmalıdır.

Yalnızca aşağıdaki türlerde çevrimiçi kumar ürünleri içeren, geçerli lisansa sahip veya yetkili kumar uygulamalarına izin verilir (her ülkede izin verilen kumar ürünü türleri için lütfen aşağıdaki tabloya bakın):

- Çevrimiçi kumarhane oyunları
- Piyangolar
- Spor bahisleri
- Günlük Fantezi Spor

Avustralya

Özet	Ayrıntılar
------	------------

Özet	Ayrıntılar
Sınırlı olarak izin verilir	Yukarıdaki başvuru ve lisanslama gereksinimlerine tabi olmak koşuluyla, aşağıdaki türlerde kumar ürünleri içeren uygulamalara izin verilir: • Spor bahisleri • Piyangolar • Günlük Fantezi Spor

Belçika

Özet	Ayrıntılar
Sınırlı olarak izin verilir	Yukarıdaki başvuru ve lisanslama gereksinimlerine tabi olmak koşuluyla, aşağıdaki türlerde kumar ürünleri içeren uygulamalara izin verilir: • Çevrimiçi kumarhane oyunları • Spor bahisleri • Piyangolar (yalnızca resmi işletmeciler)

Brezilya

Özet	Ayrıntılar
Sınırlı olarak izin verilir	Yukarıdaki başvuru ve lisanslama gereksinimlerine tabi olmak koşuluyla, aşağıdaki türlerde kumar ürünleri içeren uygulamalara izin verilir: • Piyangolar (Cixa Economa Federal tarafından yayınlanan onaylı uygulamalarla sınırlıdır) • Spor bahisleri (Yalnızca at yarışı)

Kanada

Özet	Ayrıntılar
Sınırlı olarak izin verilir	Yukarıdaki başvuru ve lisanslama gereksinimlerine tabi olmak koşuluyla, aşağıdaki türlerde kumar ürünleri içeren uygulamalara izin verilir: • Çevrimiçi Kumarhane (yalnızca resmi işletmeciler) • Spor Bahisleri (yalnızca resmi işletmeciler) • Piyangolar (yalnızca resmi işletmeciler)

Kolombiya

Özet	Ayrıntılar
Sınırlı olarak izin verilir	Yukarıdaki başvuru ve lisanslama gereksinimlerine tabi olmak koşuluyla, aşağıdaki türlerde kumar ürünleri içeren uygulamalara izin verilir: • Çevrimiçi Kumarhane • Spor Bahisleri • Piyangolar (yalnızca resmi işletmeciler)

Danimarka

Özet	Ayrıntılar
------	------------

Özet	Ayrıntılar
Sınırlı olarak izin verilir	Yukarıdaki başvuru ve lisanslama gereksinimlerine tabi olmak koşuluyla, aşağıdaki türlerde kumar ürünleri içeren uygulamalara izin verilir: - Çevrimiçi Kumarhane - Spor Bahisleri - Piyangolar - Günlük Fantezi Spor

Finlandiya

Özet	Ayrıntılar
Sınırlı olarak izin verilir	Yukarıdaki başvuru ve lisanslama gereksinimlerine tabi olmak koşuluyla, aşağıdaki türlerde kumar ürünleri içeren uygulamalara izin verilir: - Çevrimiçi Kumarhane (yalnızca resmi işletmeciler) - Spor Bahisleri (yalnızca resmi işletmeciler) - Piyangolar (yalnızca resmi işletmeciler)

Fransa

Özet	Ayrıntılar
Sınırlı olarak izin verilir	Yukarıdaki başvuru ve lisanslama gereksinimlerine tabi olmak koşuluyla, aşağıdaki türlerde kumar ürünleri içeren uygulamalara izin verilir: - Çevrimiçi Kumarhane - Spor Bahisleri - Piyangolar (yalnızca resmi işletmeciler)

Almanya

Özet	Ayrıntılar
Sınırlı olarak izin verilir	Yukarıdaki başvuru ve lisanslama gereksinimlerine tabi olmak koşuluyla, aşağıdaki türlerde kumar ürünleri içeren uygulamalara izin verilir: - Spor Bahisleri - Piyangolar (yalnızca resmi işletmeciler)

İrlanda

Özet	Ayrıntılar
Sınırlı olarak izin verilir	Yukarıdaki başvuru ve lisanslama gereksinimlerine tabi olmak koşuluyla, aşağıdaki türlerde kumar ürünleri içeren uygulamalara izin verilir: - Çevrimiçi Kumarhane - Spor Bahisleri - Piyangolar (yalnızca resmi işletmeciler veya hayır kurumu işletmecileri)

Japonya

Özet	Ayrıntılar
------	------------

Özet	Ayrıntılar
Sınırlı olarak izin verilir	Yukarıdaki başvuru ve lisanslama gereksinimlerine tabi olmak koşuluyla, aşağıdaki türlerde kumar ürünleri içeren uygulamalara izin verilir: - Spor bahisleri (yalnızca resmi işletmeciler tarafından düzenlenen at yarışı, sürat motoru yarışı, bisiklet yarışı, otomatik vitesli bisiklet yarışı ve futbol piyangosu) - Piyangolar (yalnızca resmi işletmeciler)

Meksika

Özet	Ayrıntılar
Sınırlı olarak izin verilir	Yukarıdaki başvuru ve lisanslama gereksinimlerine tabi olmak koşuluyla, aşağıdaki türlerde kumar ürünleri içeren uygulamalara izin verilir: - Çevrimiçi Kumarhane - Spor Bahisleri - Piyangolar - Günlük Fantezi Spor

Yeni Zelanda

Özet	Ayrıntılar
Sınırlı olarak izin verilir	Yukarıdaki başvuru ve lisanslama gereksinimlerine tabi olmak koşuluyla, aşağıdaki türlerde kumar ürünleri içeren uygulamalara izin verilir: - Spor Bahisleri (yalnızca resmi işletmeciler) - Piyangolar (yalnızca resmi işletmeciler)

Norveç

Özet	Ayrıntılar
Sınırlı olarak izin verilir	Yukarıdaki başvuru ve lisanslama gereksinimlerine tabi olmak koşuluyla, aşağıdaki türlerde kumar ürünleri içeren uygulamalara izin verilir: - Çevrimiçi Kumarhane - Spor Bahisleri - Piyangolar

Romanya

Özet	Ayrıntılar
Sınırlı olarak izin verilir	Yukarıdaki başvuru ve lisanslama gereksinimlerine tabi olmak koşuluyla, aşağıdaki türlerde kumar ürünleri içeren uygulamalara izin verilir: - Çevrimiçi Kumarhane - Spor Bahisleri - Piyangolar (yalnızca resmi işletmeciler)

İspanya

Özet	Ayrıntılar
------	------------

Özet	Ayrıntılar
Sınırlı olarak izin verilir	Yukarıdaki başvuru ve lisanslama gereksinimlerine tabi olmak koşuluyla, aşağıdaki türlerde kumar ürünleri içeren uygulamalara izin verilir: - Çevrimiçi Kumarhane oyunları - Spor Bahisleri - Piyangolar (yalnızca resmi işletmeciler) - Günlük Fantezi Spor

İsveç

Özet	Ayrıntılar
Sınırlı olarak izin verilir	Yukarıdaki başvuru ve lisanslama gereksinimlerine tabi olmak koşuluyla, aşağıdaki türlerde kumar ürünleri içeren uygulamalara izin verilir: - Çevrimiçi Kumarhane oyunları - Spor Bahisleri - Piyangolar (yalnızca resmi işletmeciler)

Birleşik Krallık

Özet	Ayrıntılar
Sınırlı olarak izin verilir	Yukarıdaki başvuru ve lisanslama gereksinimlerine tabi olmak koşuluyla, aşağıdaki türlerde kumar ürünleri içeren uygulamalara izin verilir: - Çevrimiçi Kumarhane oyunları - Spor Bahisleri - Piyangolar - Günlük Fantezi Spor

Amerika Birleşik Devletleri

Özet	Ayrıntılar
Sınırlı olarak izin verilir	Yukarıdaki başvuru ve lisanslama gereksinimlerine tabi olmak koşuluyla, aşağıdaki türlerde kumar ürünleri içeren uygulamalara izin verilir: - İnternet üzerinden sunulan kumarhane oyunları (Delaware, Nevada (yalnızca poker), New Jersey ve Pennsylvania'da izin verilir) - Spor bahisleri (Colorado, District of Columbia (yalnızca resmi işletmeciler), Illinois, Indiana, Iowa, Montana (yalnızca resmi işletmeciler), Nevada, New Hampshire, New Jersey, Oregon (yalnızca resmi işletmeciler), Pennsylvania, Rhode Island, Tennessee ve West Virginia'da izin verilir) - Piyangolar (yalnızca Georgia, Illinois, Kentucky, Maine, Michigan, New Hampshire, New York, North Carolina, Pennsylvania, Rhode Island ve Virginia'da eyalet kontrolündeki işletmeciler veya bağlı anlaşmalı işletmeciler) - Eyaletle bağlı olarak, günlük fantezi sporlar ABD'de kumar kapsamında düzenlenebilir. ABD'de yayınlanan tüm günlük fantezi uygulamaları aşağıdaki Günlük Fantezi Spor (DFS) Uygulamaları gereksinimlerine tabidir.

Uygun uygulamalar aşağıdaki gereksinimleri karşılamalıdır:

- Geliştirici, uygulamayı Play'de dağıtılabilmek için [başvuru sürecini başarıyla tamamlamalıdır](#);
- Uygulama, dağıtıldığı her ülkenin geçerli tüm yasalarına ve endüstri standartlarına uymalıdır;
- Geliştirici, uygulamanın dağıtıldığı her ülke veya eyalet/idari bölge için geçerli kumar lisansına sahip olmalıdır;
- Geliştirici, kumar lisansının kapsamını aşan türde bir kumar ürünü sunmamalıdır;

- Uygulama, yaşı küçük olan kullanıcıların uygulamayı kullanmasını önlemelidir;
- Uygulama, geliştirici tarafından sağlanan kumar lisansı kapsamında olmayan ülkelerden, eyaletlerden/idari bölgelerden veya coğrafi alanlardan erişimi ve kullanımı engellemelidir;
- Uygulama, Google Play'de ücretli bir uygulama olarak SUNULMAMALI ve Google Play Uygulama İçi Faturalandırma hizmetini kullanmamalıdır;
- Uygulama, Store'dan ücretsiz olarak indirilip yüklenmelidir;
- Uygulamanın AO (Yalnızca Yetişkinler İçin) veya [IARC eş değeri](#) bir derecelendirmeye sahip olması gerekir ve
- Uygulamada ve uygulamanın girişinde, sorumluluğunu bilerek kumar oynamayla ilgili bilgiler açıkça gösterilmelidir.

Gerçek Parayla Oynanan Diğer Oyunlar, Yarışmalar ve Turnuva Uygulamaları

Kumar uygulamalarıyla ilgili yukarıda belirtilen uygunluk koşullarını karşılamayan diğer tüm uygulamalarda kullanıcıların gerçek dünyada maddi değeri olan bir ödül kazanmak için gerçek para kullanarak (parayla satın alınan uygulama içi öğeler dahil) bahis oynamasını veya katılımını sağlayan ya da kolaylaştıran içerik veya hizmetlere izin verilmez. Çevrimiçi kumarhaneler, spor bahisleri, piyangolar ve para kabul eden ya da nakit veya gerçek dünyada değeri olan başka ödüller veren oyunlar buna dahil olup yalnızca bunlarla sınırlı değildir (aşağıda açıklanan Oyunlaştırılmış Bağlılık Programları gereksinimleri kapsamında izin verilen programlar hariç).

İhlal örnekleri

- Fiziksel bir ödül veya para ödülü kazanma fırsatı karşılığında para kabul eden oyunlar
- Gerçek para kullanarak turnuvalara, yarışmalara veya oyunlara katılma ya da bahis oynama konusunda kullanıcıları yönelik bir "harekete geçirici mesaj" sağlayan gezinme öğeleri veya özellikleri (ör. menü öğeleri, sekmeler, düğmeler, [web görünümüleri](#) vb.) olan uygulamalar. Örneğin, kullanıcıları para ödülü kazanma şansı yakalamaları için "BAHİS YAPIN!", "KAYDOLUN!" veya "YARIŞMAYA KATILIN!" gibi mesajlarla turnuvalara davet eden uygulamalar.
- Fiziksel ödül veya para ödülü kazanmak veya bunlar için kumar oynamak amacıyla bahisleri, uygulama içi paraları, kazançları ya da para yatırma işlemlerini kabul eden veya yöneten uygulamalar.

Oyunlaştırılmış Bağlılık Programları

Yasalarca izin verildiği ve ek kumar ya da oyun lisansı gereksinimlerine tabi olmadığı sürece, aşağıdaki Play Store uygunluk koşullarına tabi olmak üzere kullanıcıları gerçek dünyada ödül veya eşdeğeri nakitle ödüllendiren bağlılık programlarına izin verilir:

Tüm uygulamalar için (oyunlar ve oyun olmayan uygulamalar):

- Bağlılık programı avantajları, ayrıcalıkları veya ödülleri, uygulama içindeki uygun parasal işlemlere açık bir şekilde tamamlayıcı veya ikincil nitelikte olmalıdır (uygun parasal işlemin, bağlılık programından bağımsız olarak ürün veya hizmet sağlamak için gerçek bir ayrı işlem olması gerekir). Bu avantajlar, ayrıcalıklar veya ödülleri; Gerçek Parayla Kumar Oynama, Oyunlar ve Yarışmalar politikası kısıtlamalarını ihlal edecek şekilde satın alma işlemine tabi olamaz veya herhangi bir değiş tokuşla ilişkilendirilemez.
- Örneğin, uygun parasal işlemin hiçbir kısmı, bağlılık programına katılmak için bir ücreti veya bahsi temsil edemez. Ayrıca uygun parasal işlem; ürün veya hizmetlerin normal fiyatının üzerinde satın alınmasıyla sonuçlanmamalıdır.

Oyun uygulamaları için:

- Bağlılık puanları veya ödüller sadece sabit bir orana göre kazanılıp kullanılabilir. Bu oran hem uygulamada hem de programın herkese açık resmi kuralları içinde açıkça belirtilir. Ayrıca avantaj kazanımı veya kullanım değeri; oyundaki performansa ya da şansa dayalı sonuçlara göre **bahse konu edilemez, ödül olarak verilemez veya katsayısal olarak artırılmaz.**

Oyun olmayan uygulamalar için:

- Bağlılık puanları veya ödüller, aşağıdaki gereksinimleri karşılıyorsa bir yarışmayla veya şansa dayalı sonuçlarla ilişkilendirilebilir. Uygun bir parasal işlemle ilişkilendirilen avantajlar, ayrıcalıklar veya ödüller sunan bağlılık programları:
 - Programın resmi kurallarını uygulamada yayınlamalıdır.
 - Değişken, şansa dayalı veya rastgele ödül sistemleri içeren programlarda: Programın resmi kurallarında 1) ödüllerini belirlemek için sabit kazanma oranları kullanan ödül programlarının kazanma oranlarını ve 2) bu tür tüm diğer programların seçim yöntemini (örneğin ödülü belirlemek için kullanılan değişkenler) açıklayın.
 - Çekilişler veya benzer türde promosyonlar sunan bir programın resmi kurallarında her promosyon için sabit bir kazanan sayısı, katılım için sabit bir son tarih ve ödül verilme tarihi belirtmelidir.
 - Bağlılık puanı veya bağlılık ödülünün tahakkuk ve kullanım sabit oranını hem uygulamada hem de ayrıca programın resmi kurallarında açıkça belirtin.

Bağıllık programı sunan uygulama türü	Bağıllık programının oyunlaştırılması ve değişken ödüller	Sabit bir orana/programa dayalı bağıllık ödülleri	Bağıllık programının Şartlar ve Koşullar gereksinimi	Şartlar ve Koşullar'da, şansa dayalı bağıllık programının kazanma olasılıkları veya seçim yöntemi açıklanmalıdır
Oyun	İzin Verilmez	İzin Verilir	Zorunlu	Yok (Oyun uygulamalarının bağıllık programlarında şansa dayalı öğeler bulundurmasına izin verilmez)
Oyun Olmayan	İzin Verilir	İzin Verilir	Zorunlu	Zorunlu

Play'de Dağıtılan Uygulamalardaki Kumar Öğeleri veya Gerçek Parayla Oynanan Oyunlar, Yarışmalar ve Turnuvalarla ilgili Reklamlar

Kumarın, gerçek parayla oynanan oyunların, yarışmaların ve turnuvaların tanıtımını yapan reklamlar içeren uygulamalara aşağıdaki gereksinimleri karşıladıkları sürece izin verilir:

1. Uygulama ve reklam (reklamverenler dahil), reklamın gösterildiği konum için geçerli tüm yasalara ve endüstri standartlarına uymalıdır;
2. Reklam, tanıtılmakta olan kumarla ilgili tüm ürünlere ve hizmetlere ilişkin geçerli tüm yerel reklam lisans gereksinimlerini karşılamalıdır;
3. Uygulama, 18 yaşından küçük olduğu bilinen kişilere kumarla ilgili reklam göstermemelidir;
4. Uygulama, Aileler için programına kayıtlı olmamalıdır;
5. Uygulama 18 yaşından küçük bireyleri hedeflememelidir;
6. Yukarıda tanımlandığı şekilde bir Kumar Uygulamasının reklamını yapan reklamın açılış sayfasında, reklamı yapılan uygulama girişinin kendisinde veya uygulamanın içinde sorumluluğunu bilerek kumar oynamayla ilgili bilgiler açıkça gösterilmelidir;
7. Uygulamada kumar simülasyonu içeriği sağlanmamalıdır (ör. sosyal kumarhane uygulamaları, sanal slot makinesi içeren uygulamalar);
8. Uygulamada kumar, gerçek parayla oyun, piyango veya turnuva desteğine yönelik ya da tamamlayıcı işlevler (ör. bahis, ödeme, maç skoru/bahis takibi/performans takibi veya katılım fonlarının yönetimi konusunda kullanıcıya yardımcı olan işlevler);
9. Uygulama içeriği, kumar ya da gerçek parayla oynanan oyun, piyango veya turnuva hizmetlerinin tanıtımını yapmamalı veya kullanıcıları bu hizmetlere yönlendirmemelidir

Yalnızca belirtilen bölümdeki tüm gereksinimleri karşılayan uygulamalar kumar veya gerçek parayla oynanan oyun, piyango ya da turnuva reklamları içerebilir. Yukarıdaki 1-6 arası gereksinimleri karşılayan, kabul edilen Kumar Uygulamaları (yukarıda tanımlandığı gibi) veya kabul edilen Günlük Fantezi Uygulamaları (aşağıda açıklandığı gibi) kumar veya gerçek parayla oynanan oyun, piyango ya da turnuva reklamları içerebilir.

İhlal örnekleri

- Küçük yaştaki kullanıcılar için tasarlanmış olmasına rağmen kumar hizmetlerinin tanıtımını yapan reklamların gösterildiği uygulama
- Gerçek parayla kumar oynanan kumarhanelerin tanıtımını yapan veya kullanıcıları buralara yönlendiren kumarhane simülasyonu oyunu
- Bir spor bahis sitesine bağlantı veren entegre kumar reklamları içeren spor bahislerini takip etme uygulaması
- [Yanılıcı Reklamlar](#) politikamızı ihlal eden kumar reklamları (ör. kullanıcılara düğme, simge veya diğer etkileşimli uygulama içi öğeler olarak görünen reklamlar) içeren uygulamalar

Günlük Fantezi Spor (DFS) Uygulamaları

Geçerli yerel yasalarca tanımlandığı üzere günlük fantezi spor (DFS) uygulamalarına yalnızca aşağıdaki gereksinimleri karşıladıkları sürece izin verilir:

- Uygulama 1) yalnızca Amerika Birleşik Devletleri'nde dağıtılmalı veya 2) yukarıda belirtilen Kumar Uygulamaları gereksinimlerini karşılamalıdır;

- Geliştirici, uygulamayı Play'de dağıtmak için [DFS başvuru](#) sürecini başarılı bir şekilde tamamlamalı ve kabul edilmelidir;
- Uygulama, dağıtıldığı ülkeler için geçerli tüm yasalara ve endüstri standartlarına uymalıdır;
- Uygulama, yaşı küçük olan kullanıcıların uygulama içinde bahis oynamasını veya parasal işlem yapmasını engellemelidir;
- Uygulama, Google Play'de ücretli uygulama olarak satın ALINAMAMALIDIR ve Google Play Uygulama İçi Faturalandırma hizmetini kullanmamalıdır;
- Uygulama, Store'dan ücretsiz olarak indirilip yüklenmelidir;
- Uygulamanın AO (Yalnızca Yetişkinler İçin) veya IARC eş değeri bir derecelendirmeye sahip olması gerekir ve
- Uygulamada ve uygulamanın girişinde sorumluluğunu bilerek kumar oynamayla ilgili bilgiler açıkça gösterilmelidir.

Uygulama ABD'de dağıtılıyorsa aşağıdaki ek gereksinimler geçerlidir;

- Uygulama, dağıtıldığı ABD eyaleti veya ABD bölgesi için geçerli tüm yasalara ve endüstri standartlarına uymalıdır;
- Geliştirici, günlük fantezi spor uygulamaları için lisansın gerekli olduğu her ABD eyaleti veya ABD bölgesi için geçerli lisansa sahip olmalıdır;
- Uygulama, geliştiricinin günlük fantezi spor uygulamaları için gereken lisansa sahip olmadığı ABD eyaletleri veya ABD bölgelerinde kullanılmasını engellemelidir ve
- Uygulama, günlük fantezi spor uygulamalarının yasal olmadığı ABD eyaletleri veya ABD bölgelerinden kullanılmasını engellemelidir.

Yasa Dışı Faaliyetler

Yasa dışı faaliyetleri kolaylaştıran veya tanıtan uygulamalara izin verilmez.

Yaygın görülen ihlallere ilişkin bazı örnekleri aşağıda bulabilirsiniz:

- Yasa dışı uyuşturucuları veya reçeteli ilaçları reçetesiz satmayı veya satın almayı kolaylaştırma.
- Küçüklere uyuşturucu, alkol veya tütün kullanımı ya da satışını anlatma veya teşvik etme.
- Yasa dışı uyuşturucu yetiştirme veya üretmeye yönelik talimatlar.

Kullanıcı Tarafından Oluşturulan İçerik

Kullanıcı tarafından oluşturulan içerik (UGC), bir uygulamaya kullanıcının katkısı olan ve uygulamanın kullanıcılarının en az bir alt grubu tarafından görülebilen veya erişilebilen içeriktir.

UGC barındıran veya öne çıkaran uygulamalar:

- Kullanıcıların UGC'yi oluşturabilmesi veya yükleyebilmesi için önce uygulamanın kullanım şartlarını ve/veya kullanıcı politikasını kabul etmesini gerektirmelidir;
- sakıncalı içeriği ve davranışları tanımlamalı (Play'in Geliştirici Program Politikaları'na uygun şekilde) ve uygulamanın kullanım şartlarında veya kullanıcı politikalarında bunları yasaklamalıdır;
- uygulamanın barındırdığı UGC türleriyle tutarlı ve makul bir şekilde sağlam, etkili ve süren UGC moderasyonu uygulamalıdır
 - Canlı yayın uygulamalarında, sakıncalı UGC gerçek zamana mümkün olduğunca yakın bir sürede kaldırılmalıdır;
 - Artırılmış gerçeklik (AR) uygulamaları söz konusu olduğunda, UGC moderasyonu (uygulama içi raporlama sistemi dahil) hem sakıncalı AR UGC'den (ör. müstehcen bir AR görüntüsü) hem de hassas AR sabitleme konumundan sorumlu olmalıdır (ör. askeri üs gibi erişimi sınırlı bir alana veya AR sabitlemenin mülk sahibi için sorun yaratabileceği özel mülke sabitlenmiş AR içeriği);
- sakıncalı UGC'lerin bildirilmesi için kullanıcı dostu bir uygulama içi sistem sağlamalı ve yeri geldiğinde bu UGC ile ilgili gereken işlemi yapmalıdır;
- uygulamanın kullanım şartlarını ve/veya kullanıcı politikasını ihlal ederek kötüye kullananları kaldırma ya da engelleme;
- uygulama içi para kazanmanın sakıncalı kullanıcı davranışını teşvik etmesini engelleyen önlemler sağlama;

Asıl amacı sakıncalı UGC'yi öne çıkarmak olan uygulamalar Google Play'den kaldırılır. Benzer şekilde, öncelikli olarak sakıncalı UGC'nin barındırılması için kullanılan veya kullanıcılar arasında bu tür içeriğin başarılı olduğu bir yer olarak ün kazanan uygulamalar da Google Play'den kaldırılır.

Yaygın görülen ihlallere ilişkin bazı örnekleri aşağıda bulabilirsiniz:

- Sakıncalı içerikleri paylaşmayı öncelikli olarak teşvik eden ücretli özellikleri uygulamak veya bunlara izin vermek de dahil olmak üzere kullanıcılar tarafından oluşturulmuş, cinsel olarak uygunsuz içeriği tanıtmak.

- Özellikle küçüklere yönelik tehdit, taciz veya zorbalığa karşı yeterli korunma sağlamayan, kullanıcı tarafından oluşturulan içeriğe sahip uygulamalar.
- Bir uygulamanın içinde yer alan ve esas olarak taciz, kötü amaçlı saldırı veya alay etme amacıyla başka bir kişiyi taciz etmeye ya da dışlamaya yönelik yayın, yorum veya fotoğraflar.
- Kullanıcıların sakıncalı içeriklerle ilgili şikayetlerini ele alma konusunda sürekli olarak başarısız olan uygulamalar.

Onaylanmamış Maddeler

Google Play onaylanmamış maddeleri tanıtan veya satan uygulamalara, uygulamaların yasalılık iddialarını dikkate almaksızın izin vermez. Örnekler:

- [Yasaklı farmasötik ürünler ve besin takviyeleri](#) listesindeki (liste tam kapsamlı değildir) tüm maddeler
- Efedra içeren ürünler
- Zayıflama veya kilo kontrolü ile ilişkili olarak ya da anabolik steroidlerle birlikte tanıtılan ve insan koryonik gonadotropini (hCG) içeren ürünler
- Aktif farmasötik veya tehlikeli maddeler içeren bitkisel takviyeler ve besin takviyeleri
- Bir ürünün, reçeteye satılan ilaçlar veya kontrole tabi maddeler kadar etkili olduğu yönündeki iddialar da dahil olmak üzere, sağlıkla ilgili yanlış veya yanıltıcı iddialar
- Belirli bir hastalığı veya rahatsızlığı önlemek, iyileştirmek ya da tedavi etmekte kullanımının güvenli veya etkili olduğu ima edilerek pazarlanan, devlet tarafından onaylanmamış ürünler
- Hakkında herhangi bir resmi veya idari işlem ya da uyarı yapılmış ürünler
- Adları, onaylanmamış farmasötik ürünler veya besin takviyeleri ya da kontrole tabi maddelerle karıştırılabilecek düzeyde benzeyen ürünler

Denetlediğimiz onaylanmamış ve yanıltıcı farmasötik ürünler ve besin takviyeleri ile ilgili daha fazla bilgi almak için lütfen www.legitscript.com adresini ziyaret edin.

Fikri Mülkiyet

Geliştiriciler başka birinin çalışmasını kopyaladığında veya gerekli izin olmadan kullandığında o çalışmanın sahibine zarar verebilir. Başkalarının çalışmalarını adil olmayan bir şekilde kullanmayın.

Fikri Mülkiyet

Başkalarının fikri mülkiyet haklarını (ticari marka, telif hakkı, patent, ticari sır ve diğer mülkiyet hakları dahil) ihlal eden uygulamalara veya geliştirici hesaplarına izin verilmez. Fikri mülkiyet haklarının ihlalini teşvik eden veya bu tür ihlallere neden olan uygulamalara da izin verilmez.

Telif hakkı ihlali iddiası konusunda açıkça yapılan bildirimleri yanıtlıyoruz. Daha fazla bilgi edinmek veya DMCA talebinde bulunmak için lütfen [telif hakkı prosedürlerimizi](#) inceleyin.

Bir uygulamanın içinden taklit ürünler satılması veya bu tür ürünlerin satışı için tanıtım yapılmasıyla ilgili şikayette bulunmak için lütfen bir [taklit ürün bildirimi](#) gönderin.

Bir ticari marka sahibiyse ve Google Play'deki bir uygulamanın, ticari marka haklarınızı ihlal ettiğini düşünüyorsanız endişenizi gidermek için doğrudan geliştiriciye ulaşmanızı öneririz. Geliştiriciyle herhangi bir çözüme ulaşamıyorsanız lütfen bu [formu](#) kullanarak bir ticari marka şikayeti gönderin.

Uygulamanızda veya mağaza girişinizde bir üçüncü tarafın fikri mülkiyetini (marka adı, logo ve grafik öğeler gibi) kullanma iznine sahip olduğunuzu kanıtlayan yazılı dokümanınız varsa uygulamanızın fikri mülkiyet ihlalinin dolaylı reddedilmemesi için uygulamayı göndermeden önce [Google Play ekibiyle iletişime geçin](#).

Telif Hakkıyla Korunan İçeriğin Yetkisiz Kullanımı

Telif hakkını ihlal eden uygulamalara izin verilmez. Telif hakkıyla korunan içeriğin değiştirilmesi de bir ihlale neden olabilir. Geliştiricilerin, telif hakkıyla korunan içeriği kullanma haklarının olduğunu kanıtlaması gerekebilir.

Uygulamanızın işlevlerini göstermek üzere telif hakkıyla korunan içerikler kullanırken lütfen dikkatli olun. Genel olarak, en güvenli yaklaşım orijinal bir şeyler oluşturmaktır.

Genellikle yetkisiz bir şekilde veya yasal olarak geçerli bir nedenle kullanılan, telif hakkıyla korunan içeriğe ilişkin bazı örnekler aşağıda verilmiştir:

- Müzik albümleri, video oyunlar ve kitapların kapak resimleri.
- Filmler, televizyon şovları veya video oyunların pazarlama resimleri.
- Çizgi romanlar, çizgi filmler, filmler, müzik videoları veya televizyon şovlarından çizimler veya resimler.

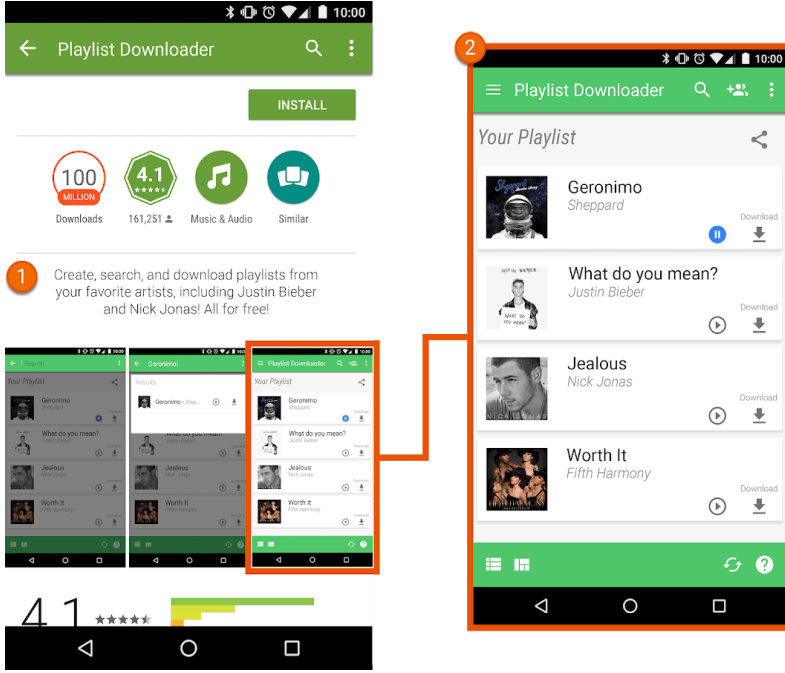
- Okul ve profesyonel spor takımlarının logoları.
- Kamuya mal olmuş bir kişinin sosyal medya hesabından alınan fotoğraflar.
- Kamuya mal olmuş kişilerin profesyonel resimleri.
- Telif hakkı korumasındaki orijinal çalışmadan ayırt edilemeyen kopyalar veya "hayran çizimleri".
- Telif hakkıyla korunan içerikten ses klipleri oynatan ses paketlerine sahip uygulamalar.
- Genel alanda olmayan kitapların tam olarak yeniden basım veya çevirileri.

Telif Hakkı İhlalini Teşvik Etme

Telif hakkı ihlaline neden olan veya bunu teşvik eden uygulamalara izin verilmez. Uygulamanızı yayınlamadan önce, telif hakkı ihlalini teşvik ediyor olup olamayacağını inceleyin ve gerekirse hukuki tavsiye alın.

Yaygın görülen ihlallere ilişkin bazı örnekleri aşağıda bulabilirsiniz:

- Kullanıcıların, telif hakkıyla korunan içeriğin yerel bir kopyasını yetkisiz bir şekilde indirmelerine olanak tanıyan akış uygulamaları.
- Kullanıcıları, geçerli telif hakkı yasasını ihlal ederek, müzik ve video da dahil olmak üzere, telif hakkıyla korunan çalışmaların akışını gerçekleştirmeye ve bu tür çalışmaları indirmeye teşvik eden uygulamalar:



- ① Bu uygulama girişindeki açıklama, kullanıcıları telif hakkıyla korunan içeriği yetkisiz bir şekilde indirmeye teşvik etmektedir.
- ② Uygulama girişindeki ekran görüntüsü, kullanıcıları telif hakkıyla korunan içeriği yetkisiz bir şekilde indirmeye teşvik etmektedir.

Ticari Marka Hak İhlali

Başkalarının ticari markalarını ihlal eden uygulamalara izin verilmez. Ticari marka, bir ürünün veya hizmetin kaynağını tanımlayan bir kelime, simge veya bunların kombinasyonudur. Ticari marka, edinildikten sonra sahibine, belirli ürün ve hizmetlerle ilgili ticari marka kullanımı için özel haklar sağlar.

Ticari marka hak ihlali, bir ürünün kaynağıyla ilgili karışıklığa neden olabilecek şekilde aynı veya benzer bir ticari markanın uygunsuz veya yetkisiz kullanımını ifade eder. Uygulamanız, başka bir tarafın ticari markalarını karışıklığa neden olabilecek şekilde kullanırsa askıya alınabilir.

Taklit Ürün

Taklit ürünler satan veya bu tür ürünlerin satışı için tanıtım yapan uygulamalara izin verilmez. Taklit ürünlerde, başka birine ait bir ticari markayla tıpatıp aynı veya ondan çok zor ayırt edilebilir ticari markalar ya da logolar yer alır. Bu ürünler, marka sahibine ait orijinal ürün gibi görünmek için o ürünün marka özelliklerini taklit eder.

Gizlilik, Yanıltma ve Cihazların Kötüye Kullanımı

Kullanıcı gizliliğini korumaya ve kullanıcılarımız için güvenli bir ortam sağlamaya büyük önem veririz. Yanıltıcı, kötü amaçlı uygulamalar veya herhangi bir ağı, cihazı ya da kişisel verileri yanlış bir şekilde veya kötüye kullanan uygulamalar kesinlikle yasaktır.

Kullanıcı Verileri

Kullanıcı verilerini (ör. bir kullanıcıdan alınan veya kullanıcı hakkında toplanan bilgiler) nasıl kullandığınız konusunda şeffaf olmalısınız. Bu gereklilik, uygulamanızın verilere erişme ve onları toplama, kullanma ve paylaşma şeklinin açıklanması, ayrıca veri kullanımının açıklanan amaçlarla sınırlandırılması anlamına gelir. Uygulamanızda kişisel veya hassas kullanıcı verileri işleniyorsa lütfen aşağıdaki "Kişisel ve Hassas Bilgiler" bölümünde yer alan ek şartlara da bakın. Bu Google Play şartları, geçerli gizlilik ve veri koruma yasalarında belirtilen şartlara ek olarak uygulanır.

Kişisel ve Hassas Bilgiler

Kişisel ve hassas kullanıcı verileri; kimliği tanımlayabilecek bilgiler, finans ve ödeme bilgileri, kimlik doğrulama bilgileri, telefon rehberi, kişiler, [cihaz konumu](#), SMS ve aramalarla ilgili veriler, mikrofon, kamera ve diğer hassas cihaz ya da kullanım verilerini içerir, ancak bunlarla sınırlı değildir. Uygulamanız hassas kullanıcı verilerini işliyorsa:

- Uygulama aracılığıyla toplanan kişisel veya hassas verilerle ilgili erişim, toplama, kullanım ve paylaşım sürecinizi, doğrudan uygulamanın özelliklerini sağlama ve iyileştirmeye ilgili amaçlarla sınırlandırmanız gerekir (ör. uygulamanın Play Store'daki açıklamasında belirtilen ve tanıtılan, kullanıcının uygulama tarafından sunulmasını beklediği işlev). Bu verileri reklam yayınlamak için kullanan uygulamalar [Reklam Politikamıza](#) uygun olmalıdır.
- Hem Play Console'da belirtilen alanda hem de uygulamanın kendi içinde bir gizlilik politikası yayınlanmalıdır. Uygulama içi açıklamalarla birlikte gizlilik politikası, uygulamanızın kullanıcıya ait verilere nasıl eriştiğini, bu verileri nasıl topladığını, kullandığını ve paylaştığını eksiksiz bir şekilde açıklamalıdır. Gizlilik politikanız, uygulamanızın eriştiği, topladığı, kullandığı ve paylaştığı kişisel ve hassas veri türlerini, ayrıca kişisel veya hassas kullanıcı verilerinin ne tür taraflarla paylaşıldığını açıklamalıdır.
- Modern kriptografi kullanarak iletme (örneğin, HTTPS üzerinden) de dahil olmak üzere tüm kişisel ve hassas kullanıcı verilerini güvenli bir şekilde işlemeniz gerekir.
- Mümkün olduğunda her zaman, [Android izinleriyle](#) korunan verilere erişmeden önce çalışma zamanı izni isteyin.
- Kişisel veya hassas kullanıcı verilerini satmayın.

Göze Çarpan Şekilde Açıklama ve Rıza Şartı

Kullanıcıların, uygulamanızın politikaya uygun özelliklerini veya işlevlerini sağlamak ya da iyileştirmek için kişisel veya hassas kullanıcı verilerinin gerekli olacağını makul biçimde tahmin etmeyebileceği durumlarda (ör. uygulamanızın arka planında veri toplanması) aşağıdaki şartları yerine getirmeniz gerekir:

Uygulamanız, verileri toplama, kullanma ve paylaşma sürecinizle ilgili bir uygulama içi açıklama sağlamalıdır. Uygulama içi açıklama:

- Yalnızca uygulama açıklamasında veya bir web sitesinde değil, uygulamanın kendi içinde de olmalıdır;
- Uygulama normal bir şekilde kullanılırken görüntülenmeli ve kullanıcının bir menüye veya ayarlara gitmesini gerektirmemelidir;
- Hangi verilere erişildiği ve hangi verilerin toplandığı açıklanmalıdır;
- Verilerin nasıl kullanılacağı ve/veya paylaşılacağı açıklanmalıdır;
- Yalnızca bir gizlilik politikasına veya hizmet şartlarına [yerleştirilemez](#) ve
- Kişisel veya hassas verilerin toplanmasıyla ilgisi olmayan diğer açıklamalara **dahil edilemez**.

Uygulama içi açıklamanız, kullanıcı onayı isteğiyle ve mümkünse çalışma zamanı istenen izinle birlikte, bu tür istekten hemen önce görünmelidir. Kullanıcı onaylayana kadar hiçbir kişisel veya hassas veriye erişemezsiniz. Uygulamanızın izin isteği:

- İzin mesajını açık ve net bir şekilde sunmalıdır;
- Kabul edilmesi için kullanıcının onay verdiğini gösteren bir eylemi (ör. kabul et seçeneğine dokunma, bir onay kutusunu işaretleme) gerektirmelidir;
- **Açıklamadan çıkılması (başka bir alana dokunma veya geri ya da ana sayfa düğmesine basma) izin olarak yorumlanmamalıdır ve**
- Otomatik kapanan veya süresi dolan mesajları kullanıcıdan izin almak için **kullanmamalıdır**.

Yaygın görülen ihlallere ilişkin bazı örnekleri aşağıda bulabilirsiniz:

- Bir kullanıcının yüklü uygulama envanterine erişen ve bu verileri yukarıdaki Gizlilik Politikası, veri işleme ve Göze Çarpan Şekilde Açıklama ve Rıza şartlarına tabi kişisel veya hassas veri olarak ele almayan bir uygulama.

- Kullanıcının telefon veya rehber verilerine erişen ve bu verileri yukarıdaki Gizlilik Politikası, veri işleme ve Göze Çarpan Şekilde Açıklama ve Rıza şartlarına tabi kişisel veya hassas veri olarak ele almayan bir uygulama.
- Kullanıcının ekranını kaydeden ve bu veriyi kişisel veya hassas veri olarak ele almayan uygulamalar bu politikaya tabidir.
- Cihaz konumu** bilgilerini toplayan ve yukarıdaki gereksinimlere uygun şekilde kullanımını açık bir şekilde ifşa etmeyen ve kullanıcının rızasını almayan bir uygulama
- Takip etme, araştırma veya pazarlama gibi amaçlarla uygulamanın arka planında kısıtlı izinleri toplayan ve yukarıdaki gereksinimlere uygun şekilde kullanımını açık bir şekilde ifşa etmeyen ve kullanıcının rızasını almayan bir uygulama.

Hassas Veri Erişimi için Özel Kısıtlamalar

Yukarıdaki gereksinimlere ek olarak, aşağıdaki tabloda belirli etkinliklere ilişkin gereksinimler açıklanmaktadır.

İşlem	Gereksinim
Uygulamanız finans veya ödeme bilgilerini ya da resmi kimlik numaralarını işliyor	Uygulamanız finansal işlemler, ödeme işlemleri veya resmi kimlik numaralarıyla ilgili kişisel ya da hassas kullanıcı verilerini hiçbir zaman herkese açık bir şekilde ifşa etmemelidir.
Uygulamanız özel telefon rehberi veya iletişim bilgilerini işliyor	Kişilerin rehberinde bulunan özel iletişim bilgilerinin izinsiz şekilde yayınlanmasına veya ifşa edilmesine izin verilmez.
Uygulamanız virüsten korunma veya güvenlik işlevlerine (ör. virüslerden, kötü amaçlı yazılımlardan korunma ya da güvenlikle ilgili özellikler) sahip	Uygulamanız, uygulama içi açıklamalarla birlikte bir gizlilik politikası yayınlayıp kullanıcıya ait hangi verileri topladığını ve ilettiğini, bunları nasıl kullandığını ve kiminle paylaştığını açıklamalıdır.

AB-ABD Gizlilik Kalkanı

Avrupa Birliği veya İsviçre kaynaklı olup bir bireyin kimliğini doğrudan veya dolaylı olarak belli eden ve Google'ın kullanılabilir hale getirdiği kişisel bilgilere ("AB Kişisel Bilgileri") erişmeniz, bu bilgileri kullanmanız veya işlemeniz halinde şunları yapmanız gerekir:

- Tüm geçerli gizlilik, veri güvenliği ve veri koruma kanunları, yönergeleri, yönetmelikleri ve kurallarına uyma;
- AB Kişisel Bilgilerini yalnızca AB Kişisel Bilgilerinin ait olduğu bireyin izin verdiği amaçlara yönelik olarak kullanma, işleme veya söz konusu bilgilere bu amaçla erişme;
- AB Kişisel Bilgilerini kaybolmaya, suistimale ve yetkisiz ya da yasa dışı erişime, ifşa edilmeye, değiştirilmeye ve yok edilmeye karşı korumak için gereken düzenlemeleri ve teknik önlemleri uygulama; ve
- Privacy Shield (Gizlilik Kalkanı) İlkeleri** 'nin gerektirdiği ile aynı koruma seviyesini sunma.

Bu koşullara uygunluğunuzu düzenli olarak izlemelisiniz. Bu şartları yerine getiremezseniz (ya da bu şartları yerine getiremeyeceğinize dair önemli bir risk varsa) hemen data-protection-office@google.com adresine e-posta göndererek durumu bize bildirmanız ve hemen ya AB Kişisel Bilgilerini işlemeyi durdurmanız ya da yeterli koruma seviyesini sağlamak için makul ve uygun adımları atmanız gerekir.

İzinler

İzin istekleri kullanıcılara mantıklı gelmelidir. Yalnızca uygulamanızın Play Store girişinde tanıtılan, hazır olan özelliklerin veya hizmetlerin kullanılabilmesi için gereken izinleri isteyebilirsiniz. Açıklanmayan, henüz uygulanmamış veya izin verilmeyen özellikler ya da amaçlar için kullanıcı veya cihaz verilerine erişim sağlayan izinleri kullanamazsınız. İzinler üzerinden erişilen kişisel veya hassas veriler hiçbir zaman satılamaz.

Kullanıcıların, uygulamanızın neden izin istediğini anlamaları için, verilere erişim izinlerini bir bağlam çerçevesinde (artımlı yetkilendirme üzerinden) isteyin. Verileri yalnızca kullanıcının izin verdiği amaçlar için kullanın. Verileri daha sonra başka amaçlar için kullanmak isterseniz, kullanıcılara bunu sormalı ve ek kullanımları kabul ettiklerinden emin olmalısınız.

Kısıtlanmış İzinler

Yukarıdakilere ek olarak, kısıtlı izinler **Tehlikeli**, **Özel** veya **İmza** olarak ifade edilen izinler olup aşağıda açıklanan ek şartlara ve kısıtlamalara tabidir:

- Kısıtlı İzinler üzerinden erişilen hassas kullanıcı veya cihaz verileri yalnızca, verilerin toplandığı uygulamadaki mevcut özellikleri veya hizmetleri sağlamak ya da iyileştirmek için gerektiğinde üçüncü taraflara aktarılabilir. Ayrıca, geçerli yasalara uymak için gereken durumlarda ya da birleşme, satın alma veya varlık satışının bir parçası olarak kullanıcılara

yasal olarak uygun şekilde bilgilendirme yaparak veri aktarımı yapabilirsiniz. Kullanıcı verilerinin başka her türlü aktarımı veya satışı yasaktır.

- Kullanıcılar Kısıtlı İzin istediğini reddederse kararlarına saygı duyun. Kullanıcılar ayrıca kritik olmayan izinlere rıza göstermeleri için manipüle edilemez veya zorlanamaz. Hassas izinlere erişim hakkı vermeyen kullanıcıların uygulamanızı kullanabilmesini sağlamak için makul ölçüde çaba göstermeniz gerekir (ör. Arama Kaydına erişimi kısıtlayan kullanıcıların manuel olarak telefon numarası girmelerine izin vermek).

Bazı Kısıtlı İzinler aşağıda açıklandığı şekilde ek şartlara tabi olabilir. Bu kısıtlamaların amacı kullanıcının gizliliğini teminat altına almaktır. Uygulamaların oldukça etkileyici veya çok önemli bir özellik sunması ve bu özelliği sağlamanın başka alternatif yöntemi olmaması gibi çok nadir durumlarda şartlarda sınırlı istisnalar yapabiliriz. Teklif edilen istisnaları değerlendirerek kullanıcıların gizliliği veya güvenliği üzerinde olası etkileri olup olmadığına bakarız.

SMS ve Arama Kaydı İzinleri

SMS ve Arama Kaydı İzinleri, [Kişisel ve Hassas Bilgiler](#) politikasına ve aşağıdaki kısıtlamalara tabi kişisel ve hassas kullanıcı verileri olarak değerlendirilir:

Kısıtlı İzinler	Gereksinim
Uygulama manifest dosyanız Arama Kaydı izin grubu (ör. READ_CALL_LOG, WRITE_CALL_LOG, PROCESS_OUTGOING_CALLS) için istekte bulunuyor	Cihazda etkin bir şekilde varsayılan Telefon veya Asistan işleyici olarak kayıtlı olmalıdır.
Uygulama manifest dosyanız, SMS izin grubu (ör. read_SMS, send_SMS, write_SMS, receive_SMS, Receive_wap_push, Receive_mms) için istekte bulunuyor	Cihazda etkin bir şekilde varsayılan SMS veya Asistan işleyici olarak kayıtlı olmalıdır.

Varsayılan SMS, Telefon veya Asistan işleyici özelliğine sahip olmayan uygulamalar manifest dosyalarında yukarıdaki izinlerin kullanımını tanımlayamaz. Bu, manifest dosyasında yer tutucu metnini içerir. Ayrıca uygulamaların, kullanıcıların yukarıdaki izinlerden herhangi birini kabul etmesini isteyebilmeleri için etkin bir şekilde varsayılan SMS, Telefon veya Asistan işleyici olarak kayıtlı olmaları ve varsayılan işleyici durumundan çıktıklarında hemen izni kullanmayı bırakmaları gerekir. İzin verilen kullanımları ve istisnaları [Yardım Merkezindeki bu sayfada](#) bulabilirsiniz.

Uygulamalar, izni (ve izin aracılığıyla oluşturulan verileri) yalnızca onaylanan temel uygulama işlevini sağlamak için kullanabilir. Temel işlev, uygulamanın asıl amacı olarak tanımlanır. Bu, temel özelliklerden oluşan bir grup da olabilir. Ancak tüm bu özelliklerin uygulamanın açıklamasında belirgin bir şekilde yer alması ve tanıtılması gerekir. Temel özelliği olmadan uygulama "çalışmaz" veya kullanışlı olmaz. Bu verilerin aktarımı, paylaşımı veya lisanslı kullanımı yalnızca uygulama içindeki temel özelliklerin sağlanması amacıyla olmalıdır ve veriler başka bir amaçla (ör. diğer uygulamaları veya hizmetleri iyileştirme, reklamcılık veya pazarlama amaçları) kullanılamaz. Arama Kaydı veya SMS ile alakalı izinlerle ilişkili veriler oluşturmak için alternatif yöntemler (başka izinler, API'ler ve üçüncü taraf kaynakları dahil) kullanamazsınız.

Konum İzinleri

[Cihaz konumu](#), [Kişisel ve Hassas Bilgiler](#) politikasına ve aşağıdaki şartlara tabi kişisel ve hassas kullanıcı verileri olarak değerlendirilir:

- Uygulamalar mevcut özellik veya hizmetlerini sağlamak için artık gerekli olmayan korunan verilere konum izinleri (ör. ACCESS_FINE_LOCATION, ACCESS_COARSE_LOCATION, ACCESS_BACKGROUND_LOCATION) ile erişemez.
- Yalnızca reklam veya analiz için kullanıcılardan asla konum izni istememelisiniz. Bu verilerin iznli kullanımının kapsamını reklam yayınlamak için genişleten uygulamalar [Reklam Politikamıza](#) uygun olmalıdır.
- Uygulamalar, konum bilgisinin kullanılmasını gerektiren mevcut özelliği veya hizmeti sağlamak için mümkün olan en dar kapsamı istemeli (yani, hassas erişim yerine genel erişim ve arka plan yerine ön plan) ve ilgili özelliğin ya da hizmetin istenen konum düzeyini gerektireceği, kullanıcılar tarafından makul ölçüde beklenebilir olmalıdır. Örneğin, ikna edici bir gerekçe sunmadan arka planda konum erişimi isteyen veya bu bilgiye erişen uygulamaları reddedebiliriz.
- Arka planda konum bilgisi yalnızca kullanıcı için faydalı ve uygulamanın temel işleviyle alakalı özellikleri sağlamak amacıyla kullanılabilir.

Bazı şartlarda uygulamaların ön plan hizmeti izni kullanarak konuma erişmesine izin verilir (uygulama yalnızca ön planda erişim iznine sahipken, örneğin "kullanımdayken"). Bunun için:

- Kullanım, kullanıcı tarafından uygulama içinde başlatılan bir işlemin devamı olarak başlatılmış olmalı ve
- kullanıcı tarafından başlatılan işlemin tasarlanan kullanım alanı uygulama tarafından tamamlandıktan hemen sonra son bulmalıdır.

Özel olarak çocuklar için tasarlanmış uygulamalar [Aileler için](#) politikasına uygun olmalıdır.

Tüm Dosyalara Erişim İzni

Bir kullanıcının cihazındaki dosyalar ve izin özellikleri, [Kişisel ve Hassas Bilgiler](#) politikasına ve aşağıdaki şartlara tabi kişisel ve hassas kullanıcı verileri olarak değerlendirilir:

- Uygulamalar yalnızca uygulamanın çalışması için kritik önem taşıyan cihaz depolama alanına erişim isteğinde bulunmalı ve kullanıcı açısından kritik uygulama işlevselliğiyle ilgili olmayan herhangi bir amaçla üçüncü taraflar adına cihaz depolama alanına erişim isteğinde bulunmamalıdır.
- R (Android 11, API Düzeyi 30) veya sonraki sürümleri çalıştıran Android cihazlar, paylaşılan depolama alanındaki erişimi yönetmek için [MANAGE_EXTERNAL_STORAGE](#) iznini gerektirir. R'yi hedefleyen ve paylaşılan depolama alanına geniş kapsamlı erişim isteyen ("Tüm dosyalara erişim") tüm uygulamalar yayınlanmadan önce uygun bir erişim değerlendirmesinden başarıyla geçmelidir. Bu izni kullanmalarına müsaade edilen uygulamalar, kullanıcılardan "Özel uygulama erişimi" ayarlarından uygulamaları için "Tüm dosyalara erişim" seçeneğini etkinleştirmelerini açıkça istemelidir. R gereksinimleri hakkında daha fazla bilgiyi bu [yardım makalesinde](#) bulabilirsiniz.

Cihazları ve Ağı Kötüye Kullanma

Kullanıcının cihazına, diğer cihazlara veya bilgisayarlara, sunuculara, ağlara, uygulama programlama arayüzlerine (API'ler) ya da cihazdaki diğer uygulamalara, Google hizmetleri de dahil ancak bunlarla sınırlı olmaksızın hizmetlere veya yetkili operatörün ağına yetkisiz bir şekilde müdahale eden, zarar veren, erişen ya da bunların çalışmasını kesintiye uğratan uygulamalara izin verilmez.

Google Play'deki uygulamalar, [Google Play için Temel Uygulama Kalitesi yönergelerinde](#) açıklanan, varsayılan Android sistem optimizasyonu gereksinimleriyle uyumlu olmalıdır.

Google Play üzerinden dağıtılan bir uygulama, Google Play'in güncelleme mekanizması dışında herhangi bir yöntem kullanarak kendisinde değişiklik yapamaz, kendini değiştiremez veya güncelleyemez. Benzer şekilde, bir uygulama Google Play dışındaki bir kaynaktan yürütülebilir kod (ör. dex, JAR, .so dosyaları) indiremez. Bu kısıtlama, bir sanal makinede çalıştırılan ve Android API'lerine sınırlı erişimi olan (bir web görünümündeki veya tarayıcıdaki JavaScript gibi) kodlar için geçerli değildir.

Güvenlik açıklarını tanıtan veya kötüye kullanan kodlara izin verilmez. Geliştiricilere bildirilen en güncel güvenlik sorunları hakkında bilgi edinmek için [Uygulama Güvenliğini İyileştirme Programı](#)'na göz atın.

Sık görülen ihlallerle ilgili bazı örnekleri aşağıda bulabilirsiniz:

- Reklam görüntüleyerek başka bir uygulamayı engelleyen veya müdahale eden uygulamalar.
- Diğer uygulamaların oynanabilirliğini etkileyen oyun hilesi uygulamaları.
- Hizmet, yazılım veya donanımlara saldırıda bulunmayı ya da güvenlik korumalarını atlatmayı kolaylaştıran veya bu konularda talimatlar sağlayan uygulamalar.
- Hizmet şartlarını ihlal edecek şekilde bir hizmete veya API'ye erişen ya da kullanan uygulamalar.
- [Beyaz listeye eklenmeye uygun olmayan](#) ve [sistem güç yönetimini](#) atlatmaya çalışan uygulamalar.
- Üçüncü taraflara proxy hizmetlerini kolaylaştıran uygulamalar bunu yalnızca uygulamanın birincil, kullanıcıya yönelik temel amacı olduğu takdirde yapabilir.
- Google Play dışındaki bir kaynaktan dex dosyaları veya yerel kod gibi yürütülebilir kodlar indiren uygulamalar ya da üçüncü taraf kodlar (ör. SDK'lar).
- Bir cihaza, önceden kullanıcının onayını almadan başka uygulamalar yükleyen uygulamalar.
- Kötü amaçlı yazılımlarla bağlantılı veya bu tür yazılımların dağıtım ya da kurulumunu kolaylaştıran uygulamalar.

Yanıltıcı Davranış

İşlevsel açıdan imkansız olmak üzere tasarlanan uygulamalarla sınırlı olmamak kaydıyla, kullanıcıları yanıltmaya çalışan veya dürüst olmayan davranışlara imkan veren uygulamalara izin verilmez. Uygulamalar, meta verinin tüm bölümlerinde işlevlerine dair doğru açıklamalar ve görüntüler/videoalar sağlamalıdır. Uygulamalar, işletim sisteminin veya başka uygulamaların işlev ya da uyarılarını taklit etmeye çalışmamalıdır. Cihaz ayarlarında yapılan değişiklikler, kullanıcının bilgisi ve onayıyla yapılmalı, kullanıcı tarafından tersine çevrilebilmelidir.

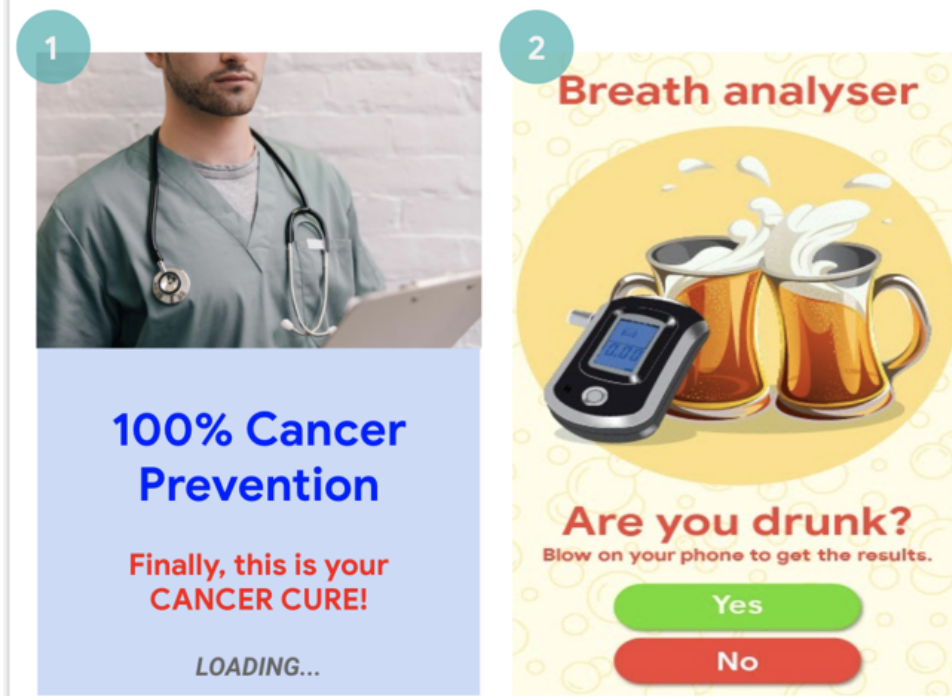
Yanıltıcı İddialar

Açıklama, başlık, simge ve ekran görüntüleri dahil olmak üzere, yanlış veya yanıltıcı bilgiler ya da iddialar içeren uygulamalara izin verilmez.

Yaygın görülen ihlallere ilişkin bazı örnekleri aşağıda bulabilirsiniz:

- İşlevlerini yanlış bir şekilde tanıtan veya doğru ve açık bir şekilde belirtmeyen uygulamalar:

- Açıklamasında ve ekran görüntülerinde bir yarış oyunu olduğunu iddia eden ama aslında araba resmi kullanan bir blok bulmaca oyunu olan uygulama.
- Virüsten korunma uygulaması olduğunu iddia eden ama yalnızca virüslerin nasıl kaldırılacağına açıkladığı bir yol gösterici metin içeren uygulama.
- Google Play'deki geçerli durum veya performanslarını yanlış gösteren geliştirici veya uygulama adları. (Ör. "Editörün Seçimi," "1 Numaralı Uygulama," "En İyi Ücretli Uygulama").
- Tıp veya sağlıkla ilgili işlevleri olan ancak yanıltıcı ya da zararlı olabilecek uygulamalar.
- Şaka, sahte, komiklik vb. olarak sunulsa bile uygulanması mümkün olmayan işlevlere sahip olduğunu iddia eden uygulamalar (ör. böcek kovma uygulamaları).
- Uygulama derecelendirmesi veya uygulama kategorisi dahil ancak bunlarla sınırlı olmamak üzere yanlış şekilde sınıflandırılmış uygulamalar.
- Oylama süreçlerini etkileyebilecek bariz bir şekilde aldatıcı içerik.
- Gerçekte olmadığı halde bir devlet kurumuyla bağlantılı olduğunu iddia eden veya gerekli yetkiye sahip olmadığı halde kamu hizmeti sağlama ya da kolaylaştırma iddiasında olan uygulamalar.
- Gerçekte olmadığı halde mevcut bir tüzel kişinin resmi uygulaması olduğunu iddia eden uygulamalar. Gerekli izinler veya haklar alınmadan "Justin Bieber Resmi Uygulaması" gibi başlıklara izin verilmez.



(1) Bu uygulama, tıbbi açıdan veya sağlıkla ilgili yanıltıcı iddialar (Kansere Çare) içeriyor

(2) Bu uygulama, uygulanması mümkün olmayan işlevlere sahip olduğunu iddia ediyor (telefonunuzu alkolmetre olarak kullanma)

Cihaz Ayarlarında Yapılan Yanıltıcı Değişiklikler

Kullanıcının bilgisi ve onayı olmadan uygulamanın dışından kullanıcının cihaz ayar veya özelliklerinde değişiklik yapan uygulamalara izin verilmez. Cihaz ayar ve özellikleri arasında sistem ve tarayıcı ayarları, yer işaretleri, kısayollar, simgeler, widget'lar ve uygulamaların ana ekranda gösterilme şekli bulunur.

Ayrıca, şunlara da izin verilmez:

- Cihaz ayarlarını veya özellikleri kullanıcının onayıyla değiştiren ancak bunu kolayca tersine çevrilebilecek bir şekilde yapmayan uygulamalar.
- Cihaz ayarlarını veya özelliklerini üçüncü taraflara hizmet etmek veya reklam sunmak amacıyla değiştiren uygulamalar veya reklamlar.
- Kullanıcıları yanlış şekilde üçüncü taraf uygulamalarını kaldırmaya veya devre dışı bırakmaya ya da cihaz ayarlarını veya özelliklerini değiştirmeye yönlendiren uygulamalar.
- Doğrulanmış bir güvenlik hizmetinin parçası olmadıkça kullanıcıları üçüncü taraf uygulamalarını kaldırmaya ya da devre dışı bırakmaya veya cihaz ayarlarını ya da özelliklerini değiştirmeye teşvik eden veya özendirilen uygulamalar.

Dürüst Olmayan Davranışlara İmkan Verme

Kimlik kartları, vatandaşlık numaraları, pasaportlar, diplomalar, kredi kartları ve sürücü belgelerinin sahtesini oluşturan veya bunların oluşturulmasını kolaylaştıran uygulamalar dahil ancak bunlarla sınırlı olmamak üzere, kullanıcıların başkalarını yanıltmasına yardımcı olan veya işlevsel açıdan herhangi bir şekilde yanıltıcı olan uygulamalara izin verilmez. Uygulamalar, uygulamanın işlevi ve/veya içeriği ile ilgili doğru başlıklar, açıklamalar ve görseller/videolar sağlamalı, kullanıcı tarafından makul ve doğru olarak beklendiği gibi çalışmalıdır.

Ek uygulama kaynakları (örneğin, oyun öğeleri) yalnızca kullanıcıların uygulamayı kullanması için gerekliyse indirilebilir. İndirilen kaynaklar tüm Google Play politikalarına uygun olmalı, ayrıca indirme işlemi başlamadan önce uygulama tarafından kullanıcılara istem gösterilerek indirme boyutu net bir şekilde açıklanmalıdır.

Bir uygulamanın "şaka", "eğlence amaçlı" (veya bu anlama gelen başka bir ifade) olduğunun iddia edilmesi, o uygulamayı politikalarımızdan muaf tutmaz.

Yaygın görülen ihlallere ilişkin bazı örnekleri aşağıda bulabilirsiniz:

- Kullanıcıları, kişisel veya kimlik doğrulama bilgilerini açıklamaları için kandırmak üzere diğer uygulamaları ya da web sitelerini taklit eden uygulamalar.
- Bireylerin veya varlıkların onayı olmadan, doğrulanmamış ya da gerçek telefon numaralarını, kişilerini, adreslerini veya kimlik bilgilerini gösteren uygulamalar.
- Bir kullanıcının coğrafi konumuna, cihaz parametrelerine veya bu farklılıkların mağaza girişinde kullanıcıya açıkça anlatılmadığı kullanıcıya dayalı diğer verilere göre temel işlevleri farklılık gösteren uygulamalar.
- Kullanıcıyı uyardırmadan (ör. "[yenilikler](#)" bölümü) ve mağaza girişini güncellemeden sürümler arasında önemli değişiklikler gösteren uygulamalar.
- İnceleme sırasında davranışı değiştirmeye veya gizlemeye çalışan uygulamalar.
- İndirme işleminden önce kullanıcıya istem göstermeyen ve indirme boyutunu açıklamayan, indirmenin içerik yayınlama ağı (CDN) ile desteklendiği uygulamalar.

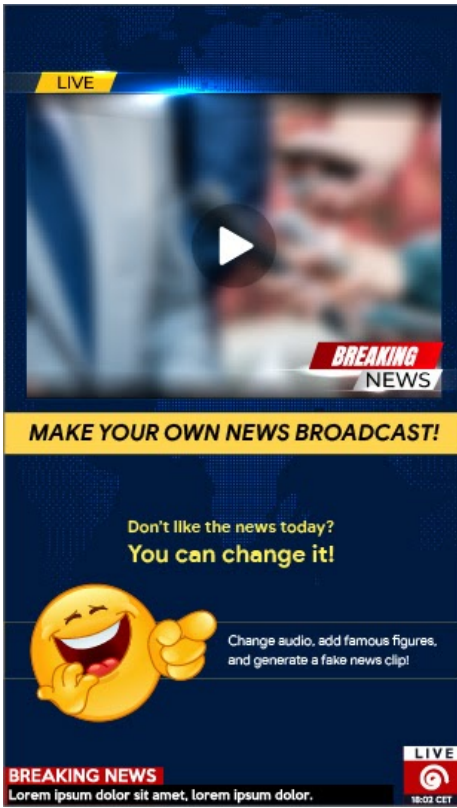
İçeriği Çarpıtılmış Medya

Görüntüler, videolar ve/veya metinler aracılığıyla yanlış veya yanıltıcı bilgi ya da iddiaların oluşturulmasına yardımcı olan veya bunların tanıtımını yapan uygulamalara izin verilmez. Hassas bir olay, politika, toplumsal konular veya kamuoyunu ilgilendiren diğer meselelerle alakalı olarak zararı dokunabilecek, bariz bir şekilde yanıltmaya veya aldatmaya yönelik görüntü, video ve/veya metinlerin tanıtımını yapmayı ya da yayılmasını sağlamayı amaçlayan uygulamalara izin verilmez.

Netliği veya kaliteyi artırmak için yapılan, konvansiyonel ve editoryal açıdan kabul edilebilir düzeyin ötesindeki düzenlemelerle medya içeriklerini çarpıtan veya değiştiren uygulamalar, ortalama bir kullanıcının medya içeriğinin değiştirildiğini net bir şekilde anlayamayabileceği durumlarda, üzerinde değişiklik yapılan medya içeriğine filigran eklemeli ya da bu değişikliği belirgin bir şekilde açıklamalıdır. Kamu yararı veya bariz hiciv ya da parodi durumlarında istisnalar söz konusu olabilir.

Yaygın görülen ihlallere ilişkin bazı örnekleri aşağıda bulabilirsiniz:

- Siyasi açıdan hassas bir etkinlik sırasındaki bir mitinge, kamuya mal olmuş bir kişiyi ekleyen uygulamalar.
- Medya üzerinde değişiklik yapabilme özelliğinin reklamını yapmak için mağaza girişinde hassas bir etkinlikten medyayı veya kamuya mal olmuş kişileri kullanan uygulamalar.
- Haber yayını süsü vermek için medya klipleri üzerinde değişiklik yapan uygulamalar.



(1) Bu uygulama, haber yayını süsü vermek için medya klipleri üzerinde değişiklik yapma ve filigran olmadan ünlü veya kamuya mal olmuş kişileri klibe ekleme işlevi sunuyor.

Yanlış Beyan

Aşağıdaki özellikleri taşıyan uygulamalara veya geliştirici hesaplarına izin verilmez:

- Herhangi bir kişinin veya kuruluşun kimliğine bürünmek ya da sahipliklerini veya ana amaçlarını yanlış beyan etmek ya da gizlemek.
- Kullanıcıları yanıltmak amacıyla düzenlenmiş faaliyetlerde bulunmak. Bu, merkez ülkelerini yanlış tanıtan veya gizleyen ya da sahte yapılar oluşturarak başka bir ülkedeki kullanıcıları hedefleyen uygulamaları veya geliştirici hesaplarını içerir, ancak bunlarla sınırlı değildir.
- Uygulama içeriğinin politika, sosyal konular veya kamuyu ilgilendiren konularla ilgili olduğu durumlarda, geliştirici veya uygulama kimliğini ya da diğer önemli ayrıntıları gizlemek veya yanlış beyan etmek için diğer uygulamalarla, sitelerle, geliştiricilerle veya diğer hesaplarla iş birliği yapmak.

Kötü Amaçlı Yazılım

Bir kullanıcıyı, kullanıcı verilerini veya bir cihazı riske atabilecek her türlü kod, kötü amaçlı yazılım kapsamına girer. Kötü amaçlı yazılımlar; Potansiyel Zararlı Uygulamalar (PHA'lar), ikili programlar veya çerçeve değişikliklerini ve truva atları, kimlik avı ve casus yazılım uygulamaları gibi kategorileri içerir, ancak bunlarla sınırlı değildir. Kategorileri sürekli güncellemekte ve yenilerini eklemekteyiz.

Kötü Amaçlı Yazılım

Kötü Amaçlı Yazılım politikamız basittir. Politikanın amacı, Google Play Store da dahil olmak üzere Android ekosistemini ve kullanıcı cihazlarını kötü amaçlı davranışlardan (ör. kötü amaçlı yazılım) korumaktır. Bu temel ilke ile kullanıcılarımıza ve Android cihazlarına güvenli bir Android ekosistemi sağlamak için çalışıyoruz.

Kötü amaçlı yazılımlar tür ve özellik açısından farklılık gösterse de genellikle aşağıdaki hedeflerden birine sahiptir:

- Kullanıcı cihazının bütünlüğünü bozarak güvenliğini ihlal etmek.
- Kullanıcı cihazının kontrolünü ele geçirmek.
- Bir saldırının, uzaktan kontrol edilebilen işlemlerle virüslü bir cihaza erişmesini, onu kullanmasını veya kötüye kullanmasını sağlamak.
- Yeterli açıklama ve izin olmadan cihazdaki kişisel verileri veya kimlik bilgilerini başka yere aktarmak.
- Virüslü cihazdan spam veya komutlar yayarak diğer cihazları ya da ağı etkilemek.

- Kullanıcıyı dolandırmak.

Bir uygulama, ikili program veya çerçeve değişikliği Potansiyel Zararlı olabileceği için, zarar verme niyetinde olmasa bile kötü amaçlı davranışların kaynağı olabilir. Bunun nedeni, uygulamaların, ikili programların veya çerçeve değişikliklerinin çeşitli değişkenlere bağlı olarak farklı şekillerde çalışabilmesidir. Dolayısıyla, bir Android cihaz için zararlı olan, başka bir Android cihaz için hiçbir risk teşkil etmeyebilir. Örneğin, Android'in son sürümünü çalıştıran bir cihaz, kötü amaçlı davranışlar gerçekleştirmek için kullanımdan kaldırılmış API'leri kullanan zararlı uygulamalardan etkilenmezken hâlâ Android'in çok eski bir sürümünü çalıştıran bir cihaz risk altında olabilir. Uygulamalar, ikili programlar veya çerçeve değişiklikleri Android cihaz ve kullanıcılarının bazıları veya tümü için açıkça risk teşkil ediyorsa kötü amaçlı yazılım ya da PHA olarak işaretlenir.

Aşağıdaki kötü amaçlı yazılım kategorileri, kullanıcıların cihazlarından nasıl yararlanıldığını anlamaları gerektiğine dair temel inancımızı yansıtır ve güçlü yenilikler ile güvenilir bir kullanıcı deneyimi sağlayan güvenli bir ekosistemi destekler.

Daha fazla bilgiyi [Google Play Protect](#) sitesinde bulabilirsiniz.

Arka kapılar

Bir cihazda istenmeyen, zararlı olabilecek, uzaktan kumanda edilen işlemlerin gerçekleştirilmesine olanak tanıyan kod.

Bu işlemler, otomatik olarak gerçekleştirilmeleri halinde uygulama, ikili program veya çerçeve değişikliğini diğer kötü amaçlı yazılım kategorilerinden birine sokacak davranışları içerebilir. Genel anlamda arka kapı, bir cihazda zararlı olabilecek bir işlemin nasıl gerçekleşebileceğini tanımlamak için kullanılır. Bu nedenle faturalandırma sahtekarlığı veya ticari casus yazılım gibi kategorilerle bire bir paralellik göstermez. Sonuç olarak bazı koşullar altında Google Play Protect tarafından güvenlik açığı olarak değerlendirilen bir arka kapı alt kümesi vardır.

Faturalandırma Sahtekarlığı

Bilinçli bir şekilde yanıltarak kullanıcıdan otomatik olarak ödeme alan kod.

Mobil faturalandırma sahtekarlığı; SMS sahtekarlığı, Telefonla arama sahtekarlığı ve Ücret sahtekarlığı olarak üçe ayrılır.

SMS sahtekarlığı

İzinsiz bir şekilde premium SMS göndermek için kullanıcılardan ödeme alan ya da mobil operatörün kullanıcıyı ücretler konusunda bilgilendirmek veya abonelikleri onaylamak amacıyla gönderdiği SMS mesajlarını ya da gizlilik sözleşmelerini gizleyerek kendi SMS etkinliklerini saklamaya çalışan kod.

Bazı kodlar, SMS gönderme davranışını teknik olarak açıklasa da SMS sahtekarlığı kapsamına giren başka davranışlarda bulunur. Örneğin, gizlilik sözleşmesinin bazı kısımlarını kullanıcıdan saklamak, bunları okunamaz hale getirmek ve mobil operatörün kullanıcıyı ücretler konusunda bilgilendirmek veya abonelikleri onaylamak amacıyla gönderdiği SMS mesajlarını yerine göre ortadan kaldırmak.

Telefon Sahtekarlığı

Kullanıcının izni olmadan premium numaraları arayarak kullanıcıdan ödeme alan kod.

İletişim Ücreti Sahtekarlığı

Kullanıcıları kandırarak cep telefonu faturaları üzerinden içerik satın almaya veya içeriklere abone olmaya yönlendiren kod.

İletişim Ücreti Sahtekarlığı, premium SMS ve premium arama hariç her türlü faturalandırmayı kapsar. Örneğin, doğrudan operatör faturalandırması, kablosuz erişim noktası (WAP) ve mobil kontör aktarımı. WAP sahtekarlığı, Ücret sahtekarlığı türleri arasında en yaygın olarak görülenlerden biridir. WAP sahtekarlığında kullanıcılar kandırılarak sessizce yüklenen, şeffaf bir Web Görünümü üzerindeki bir düğmeyi tıklamaları sağlanır. İşlem gerçekleştirildikten sonra yinelenen bir abonelik başlatılır ve kullanıcıların finansal işlemi fark etmesini önlemek için genellikle onay SMS'i veya e-postası ortadan kaldırılır.

İzleme yazılımı

Uygun bildirim yapılmadan ve yeterli izin olmadan cihazdan kişisel bilgileri aktaran ve bunun gerçekleştiğine dair kalıcı bir bildirim görüntülemeyen kod.

İzleme yazılımı uygulamaları genellikle PHA sağlayıcı dışındaki bir tarafa veri aktarır.

Bu uygulamaların kabul edilebilir biçimleri, ebeveynler tarafından çocuklarını izlemek için kullanılabilir. Ancak veriler aktarılırken kalıcı bir bildirim görüntülenmediği takdirde bu uygulamalar bir kişiyi (örneğin, eşi) habersiz olarak veya izin alınmadan takip etmek için kullanılamaz.

Yalnızca özel olarak ebeveyn (aile dahil) izleme veya kurumsal yönetim amacıyla tasarlanmış ve bu şekilde pazarlanan, politikalara uygun uygulamalar, aşağıda açıklanan gereksinimlere tam olarak uymaları koşuluyla Play Store'da izleme ve raporlama özellikleriyle dağıtılabilir.

Play Store'da dağıtılan, bir kullanıcının bir cihazda gerçekleştirdiği işlemleri gözlemleyen veya izleyen, izleme yazılımı olmayan uygulamalar en azından şu şartlara uymalıdır:

- Uygulamalar, kendilerini casusluk veya gizli izleme çözümü olarak sunmamalıdır.
- Uygulamalar, izleme davranışını saklamamalı veya gizlememeli ya da kullanıcıları, bu tür işlevlerle ilgili olarak yanlış yönlendirmeye çalışmamalıdır.
- Uygulamalar, kullanıcılara uygulamayı açıkça tanımlayan kalıcı bir bildirim ve benzersiz bir simge sunmalıdır.
- Google Play'deki uygulamalar ve uygulama girişleri, hiçbir şekilde bu şartları ihlal eden işlevleri etkinleştirmemeli veya bu tür işlevlere erişim sağlamamalıdır (ör. Google Play dışında barındırılan ve uyumlu olmayan bir APK'ya bağlantı vererek).
- Uygulamanızın, hedeflendiği yerel bölgede yasal olup olmadığını belirleme konusunda tüm sorumluluk size aittir. Yayınlandıkları konumlarda yasal olmadığı belirlenen uygulamalar kaldırılır.

Hizmet Reddi (DoS)

Kullanıcının bilgisi olmadan bir hizmet reddi (DoS) saldırısı gerçekleştiren ya da diğer sistem ve kaynaklara karşı düzenlenen dağıtılmış DoS saldırısının bir parçası olan kod.

Bu, örneğin uzak sunucular üzerinde aşırı yük oluşturmak için çok sayıda HTTP isteği göndererek gerçekleştirilebilir.

Zararlı İndirme Araçları

Kendi başına zararlı olmayan, ancak başka PHA'lar indiren kod.

Aşağıdaki durumlarda kodun zararlı bir indirme aracı olduğu söylenebilir:

- Kodun PHA'ları yaymak için oluşturulduğuna veya PHA'ları indirdiğine ya da uygulama indirip yükleyebilen kod içerdiğine dair göstergeler varsa veya
- Kod tarafından indirilen uygulamaların en az %5'i, minimum 500 gözlenen uygulama indirme eşliğine sahip PHA'lar ise (25 gözlenen PHA indirme işlemi).

Belli başlı tarayıcılar ve dosya paylaşımı uygulamaları aşağıdaki durumlarda zararlı indirme aracı olarak değerlendirilmez:

- Kullanıcı etkileşimi olmadan indirme işlemi başlatmıyorsa ve
- Tüm PHA indirme işlemleri, izin veren kullanıcılar tarafından başlatılıyorsa.

Android Dışı Tehdit

Android dışı tehditler içeren kod.

Bu uygulamalar Android cihazlara veya kullanıcılarına zarar veremez, ancak diğer platformlar için zararlı olabilecek bileşenler içerir.

Kimlik Avı

Güvenilir bir kaynaktan geliyormuş gibi görünen, kullanıcıların kimlik doğrulama veya fatura bilgilerini isteyen ve verileri üçüncü bir tarafa gönderen kod. Bu kategori, iletim halindeki kullanıcı kimlik bilgilerinin iletimini engelleyen kodlar için de geçerlidir.

Kimlik avının en yaygın hedefleri bankacılıkta kullanılan kimlik bilgileri, kredi kartı numaraları ve sosyal ağlar ile oyunlarda kullanılan online hesap kimlik bilgileridir.

Üst Düzey Ayrıcalıkları Kötüye Kullanma

Uygulamanın korumalı alanını kırarak, üst düzey ayrıcalıklar elde ederek veya güvenlikle ilgili temel işlevlere erişimi değiştirerek ya da devre dışı bırakarak sistem bütünlüğünün güvenliğini tehlikeye atan kod.

Örnek olarak şunlar verilebilir:

- Android izin modelini ihlal eden veya diğer uygulamalardan kimlik bilgilerini (ör. OAuth jetonları) çalan bir uygulama.
- Yüklemelerinin kaldırılmasını veya durdurulmalarını önleyen özellikleri kötüye kullanan uygulamalar.

- SELinux'u devre dışı bırakan bir uygulama.

Kullanıcı izni olmadan cihazları rootlayan ayrıcalık artırma uygulamaları, rootlama uygulamaları olarak sınıflandırılır.

Fidye yazılımı

Bir cihazın veya cihazdaki verilerin kontrolünü kısmen ya da büyük ölçüde ele geçiren ve kontrolü bırakmak için kullanıcıdan bir işlem gerçekleştirmesini veya ödeme yapmasını isteyen kod.

Bazı fidye yazılımları cihazdaki verileri şifreler ve verilerin şifresini çözmek için ödeme yapılmasını ister ve/veya cihaz yöneticisi özelliklerinden yararlanarak şifrelemenin sıradan bir kullanıcı tarafından kaldırılamamasını sağlar. Örnek olarak şunlar verilebilir:

- Bir kullanıcının cihazını kilitleyerek erişilemez hale getirdikten sonra kullanıcıya kontrolü geri vermek için para talep etmek.
- Cihazdaki verileri şifreledikten sonra görünürde verilerin şifresini çözmek için para talep etmek.
- Cihaz politika yöneticisinin özelliklerinden yararlanarak kullanıcı tarafından kaldırılmayı engellemek.

Asıl amacı sübvansiyonlu cihaz yönetimi olan cihazla dağıtılan kod, güvenli kilitleme ve yönetim gereksinimlerinin yanı sıra yeterli kullanıcı açıklaması ve izin gereksinimlerini başarılı bir şekilde yerine getiriyorsa fidye yazılım kategorisinin dışında tutulabilir.

Rootlama

Cihazı rootlayan kod.

Kötü amaçlı olan ve olmayan rootlama kodu arasında fark vardır. Örneğin, kötü amaçlı olmayan rootlama uygulamaları, cihazı rootlayacaklarını önceden kullanıcıya bildirir ve diğer PHA kategorileri için geçerli olan, zararlı olabilecek başka işlemler gerçekleştirmez.

Kötü amaçlı rootlama uygulamaları, cihazı rootlayacaklarını kullanıcıya bildirmez ya da bunu önceden bildirse bile diğer PHA kategorileri için geçerli olan başka işlemler de gerçekleştirir.

Spam

Kullanıcının kişilerine istenmeyen mesajlar gönderen veya cihazı bir e-posta spam aracı olarak kullanan kod.

Casus yazılım

Yeterli bildirim veya izin olmadan cihazdan kişisel verileri aktaran kod.

Örneğin, aşağıdaki bilgilerden herhangi birinin açıklama yapılmadan veya kullanıcının beklemeyeceği şekilde aktarılması casus yazılım olarak değerlendirilmek için yeterlidir:

- Kişi listesi
- SD kartta bulunan veya uygulamanın sahibi olmadığı fotoğraflar ya da diğer dosyalar
- Kullanıcı e-postasındaki içerikler
- Arama kaydı
- SMS günlüğü
- Varsayılan tarayıcının web geçmişi veya tarayıcı yer işaretleri
- Diğer uygulamaların /veri/ dizinlerindeki bilgiler.

Kullanıcıyı gizlice izleme kapsamında değerlendirilebilecek davranışlar da casus yazılım olarak işaretlenebilir. Örneğin, sesleri veya telefona gelen aramaları kaydetmek ya da uygulama verilerini çalmak.

Truva atı

Tehlikesiz gibi görünen (ör. yalnızca oyun olduğunu iddia eden bir oyun), ancak kullanıcıya karşı istenmeyen işlemler gerçekleştiren kod.

Bu sınıflandırma genellikle diğer PHA kategorileriyle birlikte kullanılır. Bir truva atı hem tehlikesiz bir bileşen hem de gizli bir zararlı bileşen içerir. Örneğin, kullanıcının haberi olmadan arka planda cihazından premium SMS mesajları gönderen bir oyun.

Yaygın Olmayan Uygulamalar ile İlgili Bir Not

Google Play Protect'in güvenli olarak değerlendirebilmek için yeterli bilgiye sahip olmadığı yeni ve nadir kullanılan uygulamalar, yaygın olmayan uygulamalar olarak sınıflandırılabilir. Bu, uygulamanın zararlı olduğu anlamına gelmez, ancak

güvenli olarak sınıflandırılabilmesi için daha fazla inceleme yapılması gerekir.

Arka Kapı Kategorisi ile İlgili Bir Not

Arka kapı kötü amaçlı yazılım kategori sınıflandırması, kodun çalışma şekline göre yapılır. Bir kodun arka kapı olarak sınıflandırılması için, otomatik olarak gerçekleştirilmesi halinde kodu diğer kötü amaçlı yazılım kategorilerinden birine sokacak bir davranışa olanak tanınması gerekir. Örneğin, bir uygulama, dinamik kod yüklemeye izin veriyor ve dinamik olarak yüklenen kod, kısa mesajları çıkartıyorsa arka kapı kötü amaçlı yazılım olarak sınıflandırılır.

Bununla birlikte, bir uygulama rastgele kod çalıştırmaya izin veriyorsa ve bu kod çalıştırma işleminin kötü amaçlı bir davranış gerçekleştirmek amacıyla eklendiğine dair bir gösterge yoksa uygulama arka kapı kötü amaçlı yazılım değil, güvenlik açığı içeren bir uygulama olarak değerlendirilir ve geliştiriciden buna yama eklemesi istenir.

Mobil İstenmeyen Yazılım

[Android ekosistemi](#) ve Google Play Store ile ilgili ilkeleri özetleyen bu politika, Google İstenmeyen Yazılım Politikası'nı temel alır. Bu ilkeleri ihlal eden yazılımlar, potansiyel olarak kullanıcı deneyimi için zararlıdır ve kullanıcıları bunlardan korumak için adımlar atarız.

Mobil İstenmeyen Yazılım

Google olarak, kullanıcıya odaklanırsak gerisinin kendiliğinden geleceğine inanırız. [Yazılım İlkelerimizde](#) ve [İstenmeyen Yazılım Politikamızda](#), kullanıcılara iyi bir deneyim sunacak yazılımlar geliştirmeye ilgili genel öneriler sunuyoruz. [Android ekosistemi](#) ve Google Play Store ile ilgili ilkeleri özetleyen bu politika, Google İstenmeyen Yazılım Politikası'nı temel alır. Bu ilkeleri ihlal eden yazılımlar, potansiyel olarak kullanıcı deneyimi için zararlıdır ve kullanıcıları bunlardan korumak için adımlar atarız.

[İstenmeyen Yazılım Politikası](#)'nda belirtildiği gibi, istenmeyen yazılımların çoğunun aynı temel özelliklerden birine veya birkaçına sahip olduğunu tespit ettik:

- Yanıltıcıdır; sunmadığı bir değer teklifinde bulunur.
- Kullanıcıları yükleme yapmaları için kandırmaya çalışır veya başka bir programın yüklemesi üzerine bindirme yapar.
- Sahip olduğu esas ve önemli işlevlerin tümü hakkında kullanıcıya bilgi vermez.
- Kullanıcının sistemini beklenmedik yöntemlerle etkiler.
- Kullanıcıların haberi olmadan kişisel bilgileri toplar veya iletir.
- Güvenli bir işlem (ör. HTTPS üzerinden iletim) yapmadan kişisel bilgileri toplar veya iletir.
- Diğer yazılımlarla birleştirilmiştir ve varlığı ifşa edilmez.

Mobil cihazlarda yazılım bir uygulama, ikili program, çerçeve değişikliği vb. biçiminde bir koddur. Yazılım ekosistemine zarar veren veya kullanıcı deneyimini bozan yazılımları engellemek için bu ilkeleri ihlal eden kodlarla ilgili gereken işlemi yaparız.

İstenmeyen Yazılım Politikası'nın kapsamını mobil yazılımları içine alacak şekilde genişletmek için aşağıda bazı eklemeler yaptık. Bu politikada olduğu gibi, Mobil İstenmeyen Yazılım politikasını yeni kötüye kullanım türlerini ele alacak şekilde hassaslaştırmaya devam edeceğiz.

Şeffaf davranış ve net açıklamalar

Tüm kodlar kullanıcıya verilen vaatleri yerine getirmelidir. Uygulamalar belirtilen tüm işlevleri sağlamalıdır. Uygulamalar kullanıcıların kafasını karıştırmamalıdır.

- Uygulamalar işlevsellik ve hedefler konusunda net olmalıdır.
- Uygulama tarafından hangi sistem değişikliklerinin yapılacağını kullanıcıya net bir şekilde açıklayın. Kullanıcıların tüm önemli yükleme seçeneklerini ve değişiklikleri inceleyip onaylamasına izin verin.
- Yazılım, kullanıcıya cihazının durumu hakkında yanlış bilgi vermemelidir (örneğin, sistem güvenliğinin kritik durumda olduğunu veya sisteme virüs bulaştığını iddia etmek).
- Reklam trafiğini ve/veya dönüşüm sayısını artırmak için tasarlanmış geçersiz etkinlikleri kullanmayın.
- Başka birinin (ör. başka bir geliştirici, şirket, varlık) veya başka bir uygulamanın kimliğine bürünerek kullanıcıları yanıltan uygulamalara izin verilmez. Uygulamanızın bağlantılı olmadığı bir kişiyle bağlantılı olduğunu veya onun tarafından yetkilendirildiğini ima etmeyin.

Örnek ihlaller:

- Reklam sahtekarlığı
- Kimliğe bürünme

Kullanıcı verilerini koruyun

Kişisel ve hassas kullanıcı verilerine erişim, bu verileri kullanma, toplama ve paylaşma konularında net ve şeffaf olun. Kullanıcı verilerini kullanırken, uygun olduğu durumlarda ilgili tüm Kullanıcı Verileri Politikalarına uyulmalı ve verileri korumak için tüm önlemler alınmalıdır.

- Üçüncü taraf hesaplarıyla ilgili veriler, e-posta, telefon numarası, yüklü uygulamalar, dosyalar, konum ve kullanıcının toplanacağını tahmin etmeyeceği diğer kişisel ve hassas veriler de dahil olmak üzere, verileri toplayıp cihazdan göndermeye başlamadan önce kullanıcılara verilerinin toplanmasına izin verme/vermeme fırsatı sunun.
- Toplanan kişisel ve hassas kullanıcı verileri, modern kriptografi kullanılarak (örneğin, HTTPS üzerinden) iletilmek de dahil olmak üzere güvenli bir şekilde işlenmelidir.
- Mobil uygulamalar da dahil olmak üzere yazılımlar, yalnızca uygulamanın işlevselliğiyle ilgili olduğunda kişisel ve hassas kullanıcı verilerini sunuculara iletmemelidir.

Örnek ihlaller:

- Veri Toplama ([Casus yazılım](#))
- Kısıtlanmış İzinlerin kötüye kullanımı

Örnek Kullanıcı Verileri Politikaları:

- [Google Play Kullanıcı Verileri Politikası](#)
- [GMS Gereksinimleri Kullanıcı Verileri Politikası](#)
- [Google API Hizmeti Kullanıcı Verileri Politikası](#)

Mobil deneyime zarar vermeyin

Kullanıcı deneyimi basit ve anlaşılması kolay olmalı, kullanıcının yapacağı net seçimlere dayanmalıdır. Kullanıcıya açık bir değer teklifi sunulmalı ve vadedilen ya da istenen kullanıcı deneyimi sekteye uğratılmamalıdır.

- Cihaz işlevlerinin kullanılabilirliğini bozmak veya aksatmak ya da kolayca kapatılmadan ve yeterli izin ve ilişkilendirme olmadan tetikleyen uygulama ortamının dışında görüntülenmek gibi beklenmedik şekillerde görüntülenen reklamları kullanıcılara göstermeyin.
- Uygulamalar diğer uygulamalara müdahale etmemeli veya cihazın kullanılabilirliğini engellememelidir
- Yeri geldiğinde uygulamayı kaldırma işlemi açık ve net olmalıdır.
- Mobil yazılım, cihaz işletim sisteminin veya diğer uygulamaların istemlerini taklit etmemelidir. Kullanıcıya diğer uygulamalardan veya işletim sisteminden gelen uyarıları, özellikle de işletim sistemindeki değişiklikleri bildirenleri engellemeyin.

Örnek ihlaller:

- Kullanımı engelleyen reklamlar
- Yetkisiz Kullanım veya Sistem İşlevselliğini Taklit Etme

Reklam Sahtekarlığı

Reklam sahtekarlığı kesinlikle yasaktır. Bir reklam ağını kandırarak trafiğin gerçek kullanıcı ilgisinden kaynaklandığına inandırmak için reklam etkileşimi oluşturmak reklam sahtekarlığıdır. Bu da bir çeşit [geçersiz trafiktir](#). Reklam sahtekarlığı, gizli reklamlar göstermek, reklamları otomatik olarak tıklamak, bilgileri değiştirmek ya da insanlar tarafından gerçekleştirilmeyen işlemlerden (örümcekler, botlar vb.) veya geçersiz reklam trafiği üretmek için tasarlanmış insan etkinliklerinden yararlanmak gibi izin verilmeyen şekillerde reklam uygulayan geliştiricilerin faaliyetlerinin bir sonucu olabilir. Geçersiz trafik ve reklam sahtekarlığı reklamverenlere, geliştiricilere ve kullanıcılara zarar vererek mobil reklam ekosisteminde uzun vadeli güven kaybına yol açar.

Yaygın görülen ihlallere ilişkin bazı örnekleri aşağıda bulabilirsiniz:

- Kullanıcı tarafından görülemeyen reklamlar oluşturan bir uygulama.
- Kullanıcının niyeti olmadan otomatik olarak reklamlara tıklama kazandıran veya hileli bir şekilde tıklama kredisi vermek için eşdeğer ağ trafiği oluşturan bir uygulama.
- Gönderenin ağından gelmeyen yüklemelerden para kazanmak için sahte yükleme ilişkilendirme tıklamaları gönderen bir uygulama.
- Kullanıcı uygulama arayüzünde değilken reklam açan bir uygulama.
- Reklam envanterinin bir uygulama tarafından olduğundan farklı gösterilmesi (örneğin, Android cihazda çalışmasına rağmen reklam ağlarına iOS cihazda çalıştığını bildiren bir uygulama; para kazanılan paket adıyla ilgili yanlış beyanda bulunan bir uygulama).

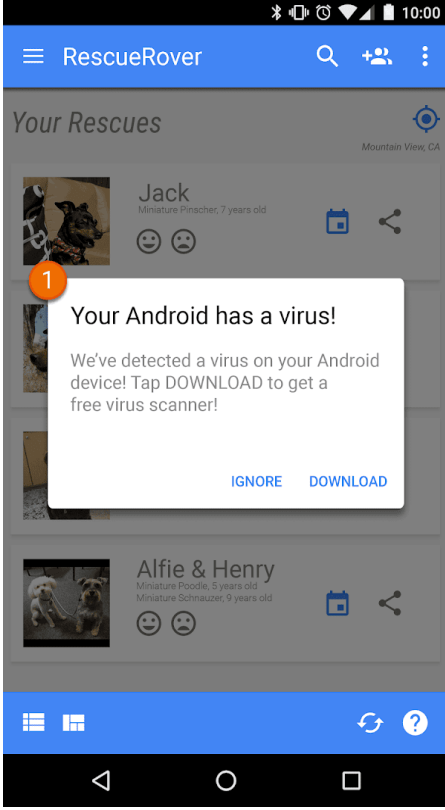
Yetkisiz Kullanım veya Sistem İşlevselliğini Taklit Etme

Bildirimler veya uyarılar gibi sistem işlevlerini taklit eden veya bunlara müdahale eden uygulamalara ya da reklamlara izin verilmez. Sistem düzeyindeki bildirimler yalnızca kullanıcılara özel fırsatları bildiren bir hava yolu uygulamasında veya

oyun içi promosyonları bildiren bir oyunda olduğu gibi uygulamanın dahili özellikleri için kullanılabilir.

Yaygın görülen ihlallere ilişkin bazı örnekleri aşağıda bulabilirsiniz:

- Bir sistem bildirimi veya uyarı üzerinden sağlanan uygulamalar ya da reklamlar:



① Bu uygulamada gösterilen sistem bildirimi, reklam sunmak için kullanılmaktadır.

Reklamlarla ilgili daha fazla örnek için lütfen [Reklam politikasına](#) bakın.

Kimliğe Bürünme

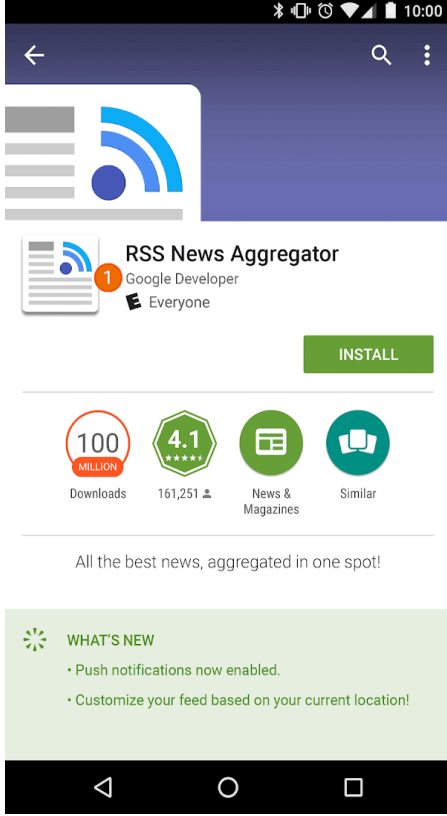
Geliştiriciler başkalarının veya uygulamalarının kimliğine büründüğünde kullanıcıları yanıltır ve geliştirici topluluğuna zarar verir. Başka birinin kimliğine bürünerek kullanıcıları yanıltan uygulamaları yasaklarız.

Kimliğe Bürünme

Başka birinin (ör. başka bir geliştirici, şirket, varlık) veya başka bir uygulamanın kimliğine bürünerek kullanıcıları yanıltan uygulamalara izin verilmez. Uygulamanızın bağlantılı olmadığı bir kişiyle bağlantılı olduğunu veya onun tarafından yetkilendirildiğini ima etmeyin. Kullanıcıları uygulamanızın başka biriyle veya başka bir uygulamayla olan ilişkisi konusunda yanıltabilecek uygulama simgeleri, açıklamalar, başlıklar veya uygulama içi öğeler kullanmamaya dikkat edin.

Yaygın görülen ihlallere ilişkin bazı örnekleri aşağıda bulabilirsiniz:

- Öyle olmadığı halde başka bir şirket/geliştirici ile ilişkisi olduğunu ima eden geliştiriciler:



① Bu uygulama için listelenen geliştirici adı, herhangi bir ilişki var olmasa bile Google ile resmi bir ilişkisi olduğu izlenimi vermektedir.

- Kullanıcıları yanlış yönlendirebilecek şekilde mevcut ürünlerin veya hizmetlerin başlıklarına ve simgelerine benzeyen uygulama başlıkları ve simgeleri:

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

Para Kazanma ve Reklamlar

Google Play, geliştiricilerin ve kullanıcıların faydalanması için aralarında ücretli dağıtım, uygulama içi ürünler, abonelikler ve reklama dayalı modellerin de bulunduğu çeşitli para kazanma stratejilerini destekler. En iyi kullanıcı deneyimini yaşatmak için bu politikalara uyulmasını zorunlu tutuyoruz.

Ödemeler

1. Google Play'deki uygulamalar ve indirilen öğeler için ücret alan geliştiriciler ödeme yöntemi olarak Google Play'in faturalandırma sistemini kullanmalıdır.
2. Google Play'de dağıtılan uygulamalar, herhangi bir uygulama işlevselliği, dijital içerik veya ürün de dahil olmak üzere özelliklere veya hizmetlere erişim için ödeme yapmayı gerektiriyor ya da ödeme kabul ediyorsa ödeme yöntemi olarak Google Play'in faturalandırma sistemini kullanmalıdır.
 - a. Google Play'in faturalandırma sisteminin kullanılmasını gerektiren uygulama özelliklerine veya hizmetlerine bazı örnekler aşağıdaki gibidir, ancak bunlarla sınırlı değildir:
 - Uygulama içinde satın alınan öğeler (ör. sanal para birimleri, ekstra canlar, ek oynama süresi, eklenti öğeleri, karakterler ve avatarlar);

- uygulama içinde satın alınan abonelik hizmetleri (ör. fitness, oyun, flört, eğitim, müzik, video ve diğer içerik aboneliği hizmetleri);
- uygulama içinde satın alınan uygulama işlevselliği veya içeriği (ör. bir uygulamanın reklamsız sürümü veya ücretsiz sürümde bulunmayan yeni özellikler) ve
- uygulama içinde satın alınan bulut yazılımı ve hizmetleri (ör. veri depolama hizmetleri, iş verimliliği yazılımları ve finansal yönetim yazılımları).

b. Google Play'in faturalandırma sistemi aşağıdaki durumlarda kullanılmamalıdır:

- ödeme esasen:

Not: Bazı pazarlarda fiziksel ürün ve/veya hizmet satan uygulamalar için Google Pay'i sunuyoruz. Daha fazla bilgi için lütfen [Google Pay geliştirici sayfamızı](#) ziyaret edin.

- fiziksel ürünlerin (ör. market ürünleri, giyim, ev eşyaları, elektronik ürünler) satın alınması veya kiralanması için yapılıyorsa;
- fiziksel hizmetlerin (ör. ulaşım hizmetleri, temizlik hizmetleri, uçak biletleri, spor salonu üyelikleri, yemek servisi, canlı etkinlikler için biletler) satın alınması için yapılıyorsa veya
- kredi kartı faturası veya kamu hizmetleri faturası (ör. kablolu televizyon ve telekomünikasyon hizmetleri) ile ilgili bir havale ise;
- ödemeler, karşılıklı ödemeleri, internet üzerinden düzenlenen açık artırmaları ve vergiden muaf bağışları içeriyorsa;
- ödeme, [Gerçek Parayla Kumar Oynama, Oyunlar ve Yarışmalar](#) politikasının [Kumar Uygulamaları](#) bölümünde tanımlandığı şekilde internette kumar oynamayı kolaylaştıran içerik veya hizmetler için yapılıyorsa;
- ödeme, Google'ın [Ödeme Merkezi İçerik Politikaları](#) kapsamında kabul edilemez sayılan ürün kategorileriyle ilgiliyse.

3. 2(b) bölümünde açıklanan uygulamaların dışındaki uygulamalar kullanıcıları Google Play'in faturalandırma sisteminden başka bir ödeme yöntemine yönlendiremez. Bu yasak, kullanıcıları aşağıdakiler aracılığıyla diğer ödeme yöntemlerine yönlendirmeyi içerir (ancak bunlarla sınırlı değildir):

- Bir uygulamanın Google Play'deki girişi;
- Satın alınabilir içerikle ilgili uygulama içi tanıtımlar;
- Uygulama içi web görünüşleri, düğmeler, bağlantılar, mesajlar, reklamlar veya diğer harekete geçirici mesajlar ve
- Kullanıcıları bir uygulamadan Google Play'in faturalandırma sistemi dışında bir ödeme yöntemine yönlendiren hesap oluşturma veya kaydolma akışları dahil olmak üzere uygulama içi kullanıcı arayüzü akışları.

4. Uygulama içi sanal para birimleri yalnızca satın alındıkları uygulama veya oyunda kullanılmalıdır.

5. Geliştiriciler, kullanıcılara uygulamalarının veya satışa sunulan uygulama içi özellikler ya da aboneliklerin şartları ve fiyatlandırması hakkında net ve doğru bilgiler vermelidir. Uygulama içi fiyatlandırma, kullanıcıya yönelik Play faturalandırma arayüzünde gösterilen fiyatlandırmayla aynı olmalıdır. Google Play'deki ürün açıklamanızda, belirli veya ek bir ücretin gerekli olabileceği uygulama içi özelliklerden bahsediliyorsa uygulama girişinizde kullanıcılara bu özelliklere erişmek için ödeme yapmaları gerektiğini açık bir şekilde bildirmelisiniz.

6. Satın alma işlemleriyle rastgele sanal öğeler almaya dair sistemler ("ganimet kutuları" dahil ancak bunlarla sınırlı olmamak üzere) sunan uygulama ve oyunlar, satın alma işleminden önce ve satın alma işlemine yakın bir zamanda bu öğeleri alabilme ihtimalini açıkça ifade etmelidir.

Abonelikler

Geliştirici olarak kullanıcıları uygulamanızda sunduğunuz abonelik hizmetleri veya içerikler konusunda yanıltmamalısınız. Gerek uygulama içi tanıtımlarda gerek başlangıç ekranlarında teklifinizi açıkça ifade etmeniz son derece önemlidir.

Uygulamanızda: Teklifiniz konusunda şeffaf olmalısınız. Bu kapsamda, teklifinizin şartları, aboneliğinizin ücreti, faturalandırma döneminizin sıklığı ve uygulamayı kullanmak için aboneliğin gerekip gerekmediği konusunda açık olmanız gerekir. Kullanıcılar bu bilgileri incelemek için fazladan işlem yapmak zorunda kalmamalıdır.

Yaygın görülen ihlallere ilişkin bazı örnekleri aşağıda bulabilirsiniz:

- Kullanıcıları her ay otomatik olarak yenilenecekleri ve ödeme alacakları konusunda bilgilendirmeyen aylık abonelikler.
- Fiyatını ağırlıklı olarak aylık ücret bazında gösteren yıllık abonelikler.
- Tam olarak yerleştirilmemiş abonelik fiyatlandırması ve şartları.
- Kullanıcıların abonelik olmadan içeriğe erişebileceğini (mümkün olduğunda) net bir şekilde göstermeyen uygulama içi tanıtımlar.

- Aboneliğin yapısını doğru yansıtmayan SKU adları. Örneğin, ödemesi otomatik olarak yinelenen bir abonelik için "Ücretsiz Deneme" ibaresinin kullanılması.

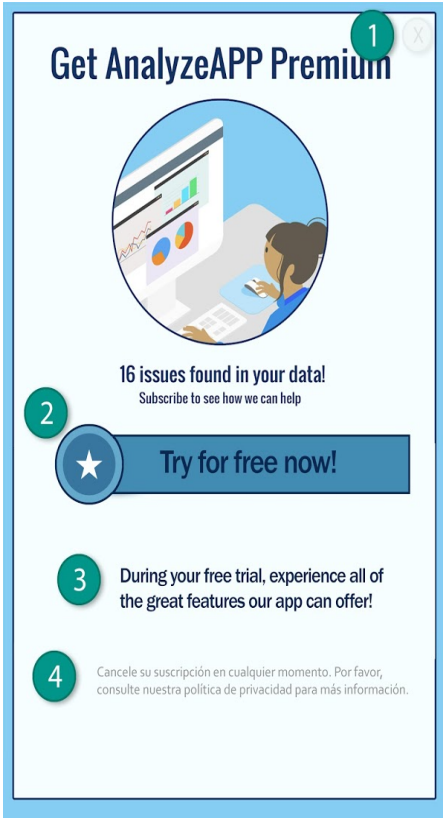
- 1 Kapatma düğmesinin net bir şekilde görünmemesi ve kullanıcıların abonelik teklifini kabul etmeden işlemlere erişebileceklerini anlayamamaları.
- 2 Teklifte fiyatlandırmanın aylık ücret üzerinden gösterilmesi ve kullanıcıların abone oldukları anda altı aylık ücret ödeyeceklerini anlayamamaları.
- 3 Teklifte yalnızca tanıtım fiyatının gösterilmesi ve kullanıcıların, tanıtım süresinin sonunda kendilerinden otomatik olarak ne kadar ödeme alınacağını anlayamamaları.
- 4 Kullanıcıların teklifin tamamını anlayabilmeleri için teklif, şartlar ve koşullar ile aynı dile yerleştirilmelidir.

Ücretsiz Denemeler ve Tanıtım Amaçlı Teklifler

Kullanıcılar aboneliğine kaydolmadan önce: Teklifinizin şartlarını (ör. süre, fiyatlandırma, erişilebilir içerik veya hizmetlerin tanımı) açık ve doğru bir şekilde anlatmalısınız. Kullanıcılarınızı ücretsiz denemenin nasıl ve ne zaman ücretli aboneliğe dönüşeceği, ücretli aboneliğin fiyatı ve ücretli aboneliğe geçmek istemeyen kullanıcıların aboneliklerini iptal edebilecekleri konusunda bilgilendirdiğinizden emin olun.

Yaygın görülen ihlallere ilişkin bazı örnekleri aşağıda bulabilirsiniz:

- Ücretsiz denemenin veya tanıtım fiyatının ne kadar süre boyunca geçerli olacağını net bir şekilde açıklamayan teklifler
- Teklifin süresi bittikten sonra kullanıcının otomatik olarak ücretli aboneliğe kaydedileceğini net bir şekilde açıklamayan teklifler.
- Kullanıcıların deneme olmadan içeriğe erişebileceğini (mümkün olduğunda) net bir şekilde göstermeyen teklifler.
- Tam olarak yerleştirilmemiş teklif fiyatlandırması ve şartları.



- ① Kapatma düğmesinin net bir şekilde görünmemesi ve kullanıcıların ücretsiz denemeye kaydolmadan işlevlere erişebileceklerini anlayamamaları.
- ② Teklifin ücretsiz denemeyi vurgulaması ve kullanıcıların, deneme süresinin sonunda kendilerinden otomatik olarak ödeme alınacağını anlayamamaları.
- ③ Teklifte deneme süresinden bahsedilmemesi ve kullanıcıların abonelik içeriğine ne kadar süre boyunca ücretsiz olarak erişebileceklerini anlayamamaları.
- ④ Kullanıcıların teklifin tamamını anlayabilmeleri için teklif, şartlar ve koşullar ile aynı dile yerleştirilmelidir.

Abonelik Yönetimi ve İptali

Geliştirici olarak, kullanıcıların aboneliklerini nasıl yönetebileceklerini veya iptal edebileceklerini uygulamanızda açıkça belirtmeniz gerekir.

Kullanıcılarınıza abonelik, iptal ve geri ödeme politikalarınızdaki değişiklikleri bildirme ve politikaların geçerli yasalara uygun olmasını sağlama konusunda sorumluluk size aittir.

Reklamlar

Yanıtıcı olan veya kullanımı engelleyen reklamların gösterildiği uygulamalara izin verilmez. Reklamlar, yalnızca bunları sunan uygulama içinde görüntülenmelidir. Uygulamanızda yayınlanan reklamlar, uygulamanızın bir parçası olarak kabul edilir. Uygulamanızda gösterilen reklamlar tüm politikalarımıza uygun olmalıdır. Kumar reklamları ile ilgili politikalar için [burayı](#) tıklayın.

Konum Verilerinin Reklamlar için Kullanımı

İzne dayalı cihaz konum verilerini reklam yayınlamak için kullanan uygulamalar, [Kişisel ve Hassas Bilgiler](#) politikasına tabi olup aşağıdaki şartlara uymakla yükümlüdür:

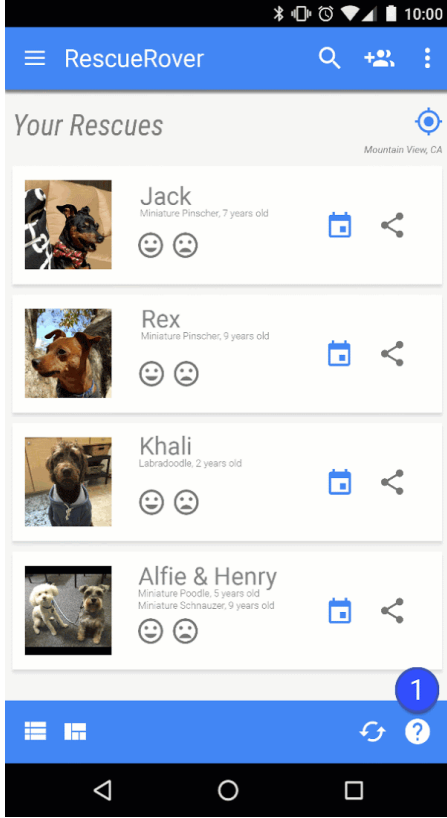
- İzne dayalı cihaz konum verileri reklam için kullanılacak veya toplanacaksa bu durum kullanıcıya açıkça bildirilmeli ve uygulamanın zorunlu gizlilik politikasında yer almalıdır. Bu kapsamda, konum verilerinin kullanımını ele alan alakalı reklam ağı gizlilik politikalarına da bağlantı verilmelidir.
- [Konum İzinleri](#) gereksinimleri uyarınca, konum izinleri yalnızca uygulamanızdaki mevcut özellikleri veya hizmetleri sağlamak için istenebilir, salt reklam kullanımı için istenemez.

Yanıtıcı Reklamlar

Reklamlar, herhangi bir uygulamanın kullanıcı arayüzünü, bir işletim sisteminin bildirim ya da uyarı öğelerini taklit etmemeli veya bunların kimliğine bürünmemelidir. Her bir reklamı hangi uygulamanın sunduğu kolayca anlaşılmalıdır.

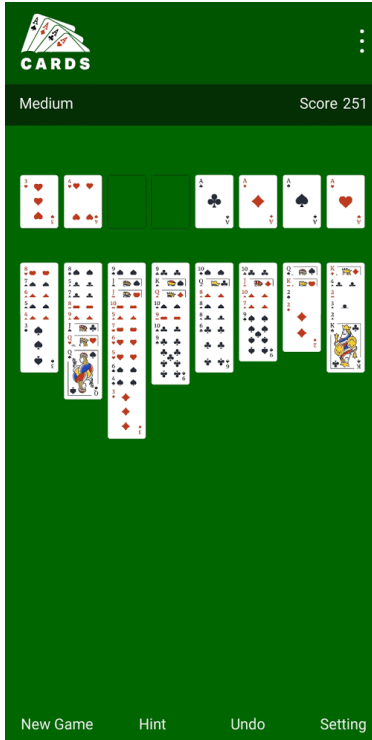
Yaygın görülen ihlallere ilişkin bazı örnekleri aşağıda bulabilirsiniz:

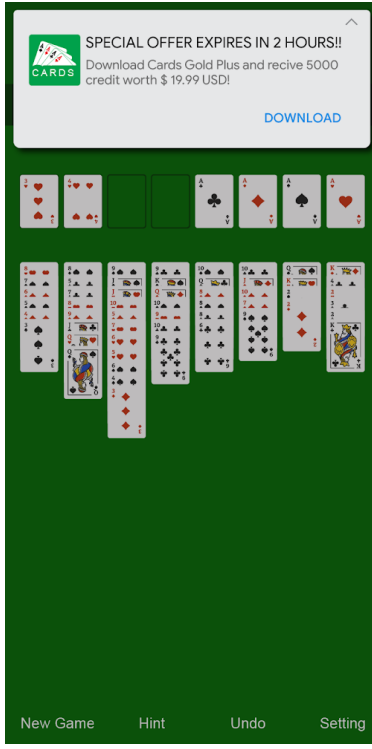
- Bir uygulamanın kullanıcı arayüzünü taklit eden reklamlar:



① Bu uygulamadaki soru işareti simgesi, kullanıcıyı harici bir açılış sayfasına yönlendiren bir reklamdır.

- Sistem bildirimlerini taklit eden reklamlar:





Yukarıdaki örneklerde, çeşitli sistem bildirimlerini taklit eden reklamlar gösterilmektedir.

Kilitli Ekrandan Para Kazanma

Uygulamanın tek amacının ekran kilidi işlevi görmek olmaması halinde uygulamalar bir cihazın kilitli ekranından para kazandıran reklam veya özellikleri kullanamaz.

Kullanımı Engelleyen Reklamlar

Kullanımı engelleyen reklamlar, kullanıcılara beklenmedik şekillerde gösterilen, yanlışlıkla tıklamaya yol açabilen veya cihaz işlevlerinin kullanılabilirliğini bozabilen ya da aksatabilen reklamlardır.

Uygulamanız, bir uygulamayı tam anlamıyla kullanabilmeleri için kullanıcıları bir reklamı tıklamaya veya reklamcılık amacıyla kişisel bilgilerini vermeye zorlayamaz. Geçiş reklamları sadece bunları sunan uygulama içinde görüntülenebilir. Uygulamanız görüntülü ağ geçiş reklamları veya normal kullanımı aksatan başka reklamlar görüntülüyorsa bunların ceza olmadan kolayca kapatılabilmesi gerekir.

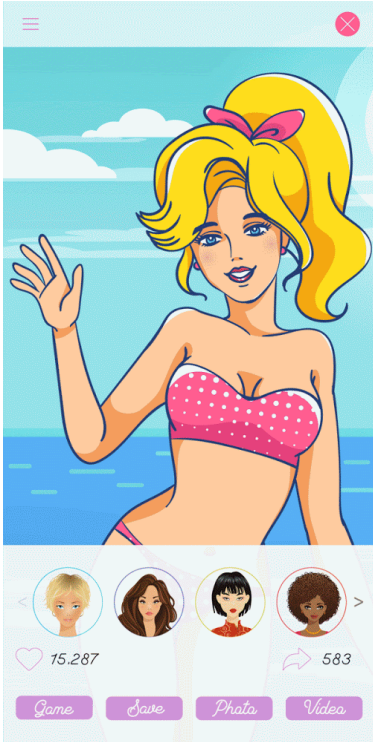
Yaygın görülen ihlallere ilişkin bazı örnekleri aşağıda bulabilirsiniz:

- Ekranın tamamını kaplayan veya normal kullanımı aksatan ve reklamı kapatmak için açık bir yol sağlamayan reklamlar:

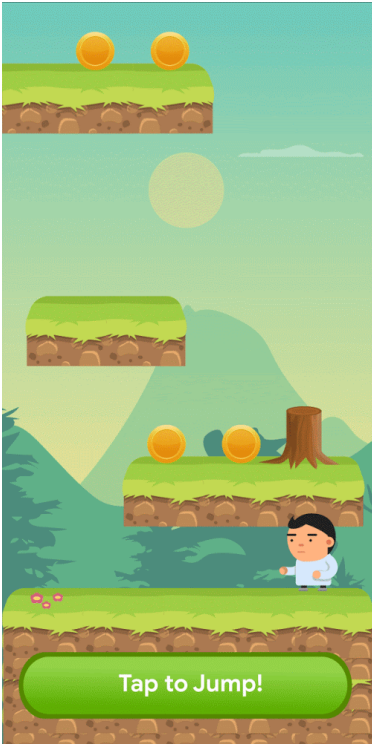


① Bu reklamın bir kapat düğmesi yoktur.

- Sahte bir kapatma düğmesi kullanarak veya uygulamada kullanıcıların genellikle başka bir işlev için dokunduğu alanlarda aniden reklam göstererek kullanıcıyı tıklamaya zorlayan reklamlar.



Sahte kapatma düğmesi kullanan bir reklam



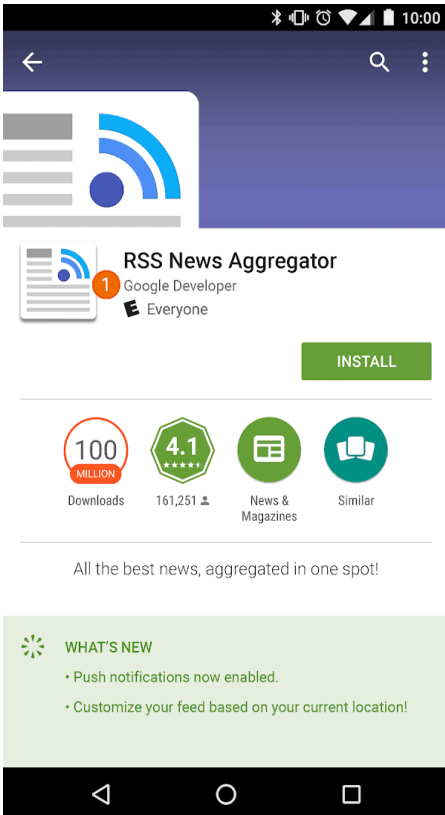
Kullanıcının uygulama içi işlevler için dokunmaya alışkın olduğu bir alanda aniden görünen bir reklam

Uygulamaları, Üçüncü Taraf Reklamlarını veya Cihazın İşlevlerini Aksatma

Uygulamanızla ilişkili reklamlar başka uygulamalar, reklamlar veya sistem ya da cihaz düğmeleri ve bağlantı noktaları da dahil olmak üzere cihazın çalışmasını aksatmamalıdır. Bunlar arasında yer paylaşimleri, tamamlayıcı öğelerin işlevleri ve widget haline getirilmiş reklam birimleri bulunur. Reklamlar, yalnızca bunları sunan uygulama içinde görüntülenmelidir.

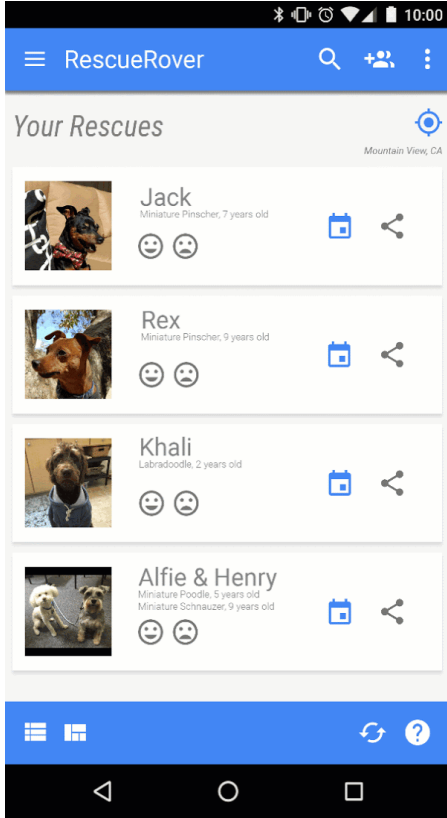
Yaygın görülen ihlallere ilişkin bazı örnekleri aşağıda bulabilirsiniz:

- Sunumu yapan uygulamanın dışında görüntülenen reklamlar:



Açıklama: Kullanıcı, bu uygulamadan ana ekrana gider ve aniden ana ekranda bir reklam görüntülenir.

- Ana ekran düğmesi veya açık bir şekilde uygulamadan çıkış için tasarlanmış diğer özelliklerin tetiklediği reklamlar.

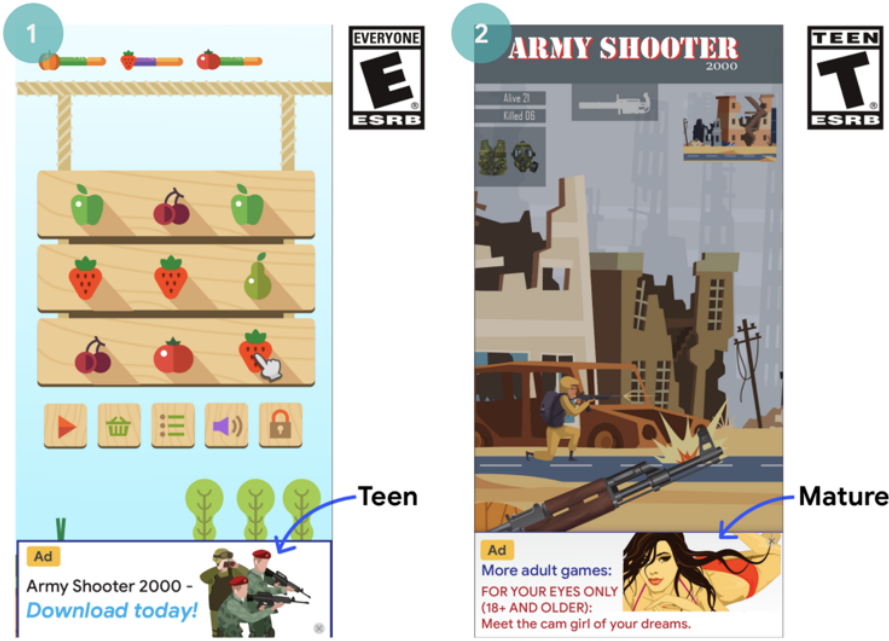


Açıklama: Kullanıcı uygulamadan çıkmayı ve ana ekrana gitmeyi dener, ancak bunun yerine bir reklam görünür ve beklenen akış kesintiye uğrar.

Uygunsuz Reklamlar

İçeriğin kendisi politikalarımızla bir şekilde uyumlu olsa bile, uygulamanızda gösterilen reklamlar da uygulamanın hedef kitlesine uygun olmalıdır.

Aşağıda, yaygın görülen bir ihlale ilişkin örneği bulabilirsiniz:



- ① Bu reklam (Genç) bu uygulamanın hedef kitlesi için uygunsuzdur (7+)
- ② Bu reklam (Erişkin) bu uygulamanın hedef kitlesi için uygunsuzdur (12+)

Android Reklam Kimliğinin Kullanımı

Google Play Hizmetleri 4.0 sürümü, reklam ve analiz sağlayıcıları tarafından kullanılmak üzere yeni API'ler ve bir kimlik sunar. Bu kimliğin kullanımıyla ilgili şartlar aşağıdadır.

- **Kullanım.** Android reklam tanımlayıcısı sadece reklam ve kullanıcı analizi için kullanılmalıdır. Kimliğin her erişiminde "İlgi alanına dayalı reklamları devre dışı bırak" veya "Reklam Kişiselleştirme'yi kapat" ayarının durumu doğrulanmalıdır.
- **Kimliği tanımlayabilecek bilgiler veya diğer tanımlayıcılarla olan ilişki**
 - Reklam kullanımı: Reklam tanımlayıcısı herhangi bir reklamcılık amacıyla kalıcı cihaz tanımlayıcılarla (ör. SSAID, MAC adresi, IMEI vb.) ilişkilendirilemez. Reklam tanımlayıcısı yalnızca kullanıcının açık izni olduğunda kimlik bilgileriyle ilişkilendirilebilir.
 - Analytics kullanımı: Reklam tanımlayıcısı yalnızca kullanıcının açık izni olduğunda kimlik bilgileriyle bağlantılı hale getirilebilir veya kalıcı cihaz tanımlayıcılarla (ör. SSAID, MAC adresi, IMEI vb.) ilişkilendirilebilir.
- **Kullanıcıların seçimlerine saygı.** Sıfırlanırsa kullanıcının açık izni olmadan yeni bir reklam tanımlayıcısı bir önceki reklam tanımlayıcısıyla veya önceki reklam tanımlayıcısından türetilen verilerle ilişkilendirilmemelidir. Ayrıca, bir kullanıcının "İlgi alanına dayalı reklamları devre dışı bırak" veya "Reklam Kişiselleştirme'yi kapat" ayarına uymanız gerekir. Bir kullanıcı bu ayarı etkinleştirmişse, reklam amaçlı olarak veya ilgi alanına dayalı reklamlarla kullanıcıları hedeflemek için kullanıcı profilleri oluşturmak üzere reklam tanımlayıcısını kullanamazsınız. İzin verilen etkinlikler; içeriğe dayalı reklamcılık, sıklık sınırı, dönüşüm izleme, rapor gönderme, güvenlik ve sahtekarlık algılamasını içerir.
- **Kullanıcılara karşı şeffaflık.** Reklam tanımlayıcısının toplanması, kullanılması ve bu şartlara bağlılık gibi konuların yasal olarak yeterli düzeyde bir gizlilik bildirimi aracılığıyla kullanıcılara açıklanması gerekir. Gizlilik standartlarımız hakkında daha fazla bilgi edinmek için lütfen [Kullanıcı Verileri](#) politikamıza bakın.
- **Kullanım şartlarına uyma.** İşiniz gereği paylaşabileceğiniz taraflar dahil olmak üzere, reklam tanımlayıcısı sadece bu şartlara uygun şekilde kullanılabilir. Google Play'e yüklenen veya Google Play'de yayınlanan tüm uygulamalarda, reklam amaçlarıyla diğer cihaz tanımlayıcılarının yerine reklam kimliğinin (cihazda varsa) kullanılması gerekir.

Aile Reklam Programı

Uygulamanızda reklam yayınluyorsanız ve uygulamanızın hedef kitlesi, [Aile Politikası](#)'nda açıklandığı gibi yalnızca çocukları içeriyorsa aşağıdaki Reklam SDK'sı sertifikasyon şartları da dahil olmak üzere içerik üretici onayı açısından Google Play politikalarıyla uyumlu olan reklam SDK'larını kullanmanız gerekir. Uygulamanızın hedef kitlesi hem çocukları hem de daha büyük kullanıcıları içeriyorsa yaş filtreleme önlemleri uygulayarak çocuklara gösterilen reklamların yalnızca bu içerik üretici onaylı reklam SDK'larının birinden geldiğinden emin olmanız gerekir. Aileler için programında yer alan uygulamaların yalnızca içerik üretici onaylı reklam SDK'larını kullanması zorunludur.

Yalnızca çocuklara reklam yayınlamak için reklam SDK'ları kullanırken Google Play onaylı reklam SDK'larının kullanılması zorunludur. Bir reklam SDK'sının Google Play'de içerik üretici onayı olmadan kullanılmasına aşağıdaki durumlarda izin

verilir, ancak reklam içeriğinizin ve veri toplama uygulamalarınızın Play'in [Kullanıcı Verileri Politikası](#) ve [Aile Politikası](#)'na uymasını sağlamak sizin sorumluluğunuzdadır:

- Uygulamalarınızın veya sahip olduğunuz diğer medya ve ürünlerin çapraz tanıtımını yönetmek için SDK'ları kullandığınız Şirket İçi Reklam
- Envanter yönetimi için SDK'ları kullandığınız reklamverenlerle doğrudan sunulan anlaşmalar yapmak

Reklam SDK'sı Sertifikasyon Şartları

- Sakıncalı reklam içeriği ve davranışları tanımlayıp bunları reklam SDK'sının şartları veya politikalarında yasaklayın. Tanımlar Play'in Geliştirici Program Politikaları'na uygun olmalıdır.
- Reklam öğelerinizi yaş gruplarına uygunluğa göre derecelendirecek bir yöntem oluşturun. Yaş grupları arasında en azından Herkes için ve Yetişkinlere yönelik gruplar bulunmalıdır. Derecelendirme yöntemi, Google'in aşağıdaki başvuru formunu dolduran SDK'lara sağladığı yöntemle tutarlı olmalıdır.
- Yayıncıların, istek bazında veya uygulama bazında reklam sunumu için çocuklara yönelik olarak değerlendirilme isteğinde bulunmalarına izin verin. Bu tür değerlendirmeler, geçerli yasa ve yönetmeliklere (ör. [ABD Çocukların Çevrimiçi Gizliliğini Koruma Yasası \(COPPA\)](#) ve AB [Genel Veri Koruma Yönetmeliği \(GDPR\)](#)) uygun olmalıdır. Google Play, çocuklara yönelik olarak değerlendirilme kapsamında reklam SDK'larının kişiselleştirilmiş reklamları, ilgi alanına dayalı reklamcılığı ve yeniden pazarlamayı devre dışı bırakmasını şart koşar.
- Yayıncıların [Play'in Aile Reklamları ve Para Kazanma politikasına](#) uygun reklam biçimleri seçmesine ve [Öğretmen Onaylı programının](#) gereksinimini yerine getirmesine izin verin.
- Çocuklara reklam yayınlanmak için gerçek zamanlı teklif verme seçeneğini kullanırken reklam öğelerinin incelendiğinden ve gizlilik göstergelerinin teklif verenlere iletiğinden emin olun.
- Google'a reklam SDK'sının tüm sertifikasyon şartlarına uyduğunu doğrulamak için yeterli bilgiyi sağlayın (aşağıdaki [başvuru formunda](#) yer alan bilgiler gibi) ve daha sonra gönderilecek bilgi isteklerine zamanında yanıt verin.

Not: Reklam SDK'ları, yayıncıları için geçerli olabilecek, çocuklarla ilgili tüm mevzuatlara ve yönetmeliklere uygun reklam sunmayı desteklemelidir.

Çocuklara reklam sunarken reklam sunma platformları için uyumlulaştırma şartları:

- Yalnızca Play onaylı reklam ağlarını kullanın veya uyumlulaştırma ağlarından sunulan tüm reklamların bu şartlara uymasını sağlamak için gerekli güvenlik önlemlerini uygulayın ve
- reklam içeriğinin derecelendirmesini ve çocuklara yönelik geçerli değerlendirmeleri belirtmek için uyumlulaştırma platformlarına gereken bilgileri sağlayın.

Geliştiriciler [içerik üretici onaylı SDK'ların listesini](#) burada bulabilir.

Geliştiriciler ayrıca bu [başvuru formunu](#) içerik üretici onayı almak isteyen reklam SDK'larıyla paylaşabilir.

Mağaza Girişi ve Tanıtım

Uygulamanızın tanıtımı ve görünürlüğü mağazanın kalitesini önemli ölçüde etkiler. Spam içerikli mağaza girişlerinden, düşük kaliteli tanıtımlardan ve Google Play'de uygulama görünürlüğünü yapay olarak artıracak çalışmalardan kaçının.

Uygulama Tanıtımı

Kullanıcılar veya geliştirici ekosistemi için yanıltıcı ya da zararlı olabilecek tanıtımlara izin verilmez. Bu nedenle, uygulamalar doğrudan veya dolaylı olarak bu tür tanıtımlarda bulunamaz ya da bu tür tanıtımlardan fayda sağlayamaz. Yanıltıcı veya zararlı davranışlar bulunan uygulamalar şunları içerir:

- Sistem bildirimleri ve uyarılarına benzeyen bildirimler de dahil olmak üzere, web sitelerinde, uygulamalarda veya diğer mülklerde yanıltıcı reklamlar kullanma.
- Kullanıcıların bilerek ve isteyerek gerçekleştirdikleri eylemler dışında, kendilerini Google Play'e yönlendiren veya uygulamaların indirilmesine neden olan tanıtım veya yükleme taktikleri.
- Kullanıcıların isteği dışında SMS gönderilerek yapılan tanıtım.

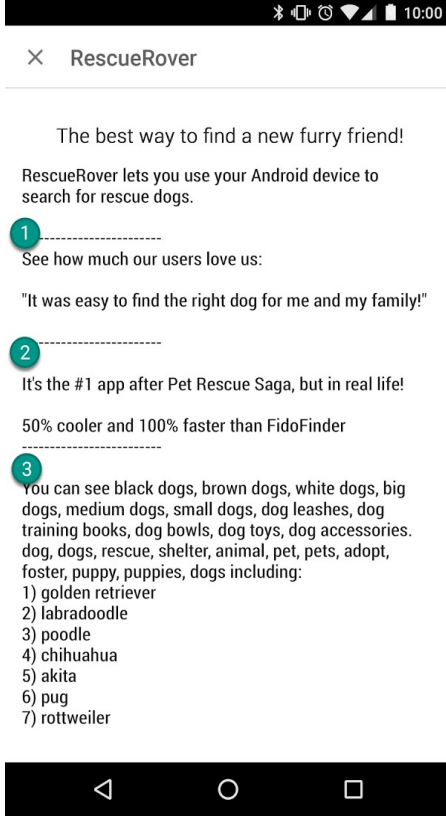
Uygulamanızla ilişkilendirilen reklam ağlarının veya satış ortaklarının bu politikaları uymalarını ve yasaklanmış tanıtım yöntemlerini kullanmamalarını sağlamak sizin sorumluluğunuzdadır.

Meta veri

Uygulama açıklaması, geliştirici adı, başlık, simge, ekran görüntüleri ve tanıtım görselleri dahil ancak bunlarla sınırlı olmamak üzere yanıltıcı, yanlış biçimlendirilmiş, açıklayıcı olmayan, alakasız, aşırı veya uygunsuz meta veriler içeren uygulamalara izin verilmez. Geliştiriciler uygulamalarıyla ilgili net ve iyi yazılmış bir açıklama sağlamalıdır. Uygulamanın açıklamasında ilişkilendirilmemiş veya anonim kullanıcı görüşlerine de izin verilmez.

Burada belirtilen gereksinimlere ek olarak, bazı Play Geliştirici Politikaları kapsamında başka meta veri bilgileri de sağlamanız gerekebilir.

Yaygın görülen ihlallere ilişkin bazı örnekleri aşağıda bulabilirsiniz:



- 1) İlişkilendirilmemiş veya Anonim Kullanıcı görüşleri
- 2) Uygulamaların veya markaların veri karşılaştırması
- 3) Kelime blokları ve dikey/yatay kelime listeleri

Girişinizdeki uygunsuz metin, resim veya videolarla ilgili bazı örnekleri burada bulabilirsiniz:

- Müstehcen içerik barındıran görüntü ve videolar. İster çizim ister gerçek olsun göğüs, kalça, genital bölge veya vücutla ilgili fetiş olan diğer bölgeleri içeren müstehcen görüntülerden kaçınınız.
- Uygulamanızın mağaza girişinde küfürlü, kaba veya genel kitleye uygun olmayan başka bir dil kullanmak.
- Uygulama simgeleri, tanıtım resimleri veya videolarda belirgin bir şekilde gösterilen sansürlenmemiş şiddet.
- Yasa dışı uyuşturucu kullanımı tasviri. EBBS (Eğitimsel, Belgesel, Bilimsel veya Sanatsal) bile olsa içeriğin mağaza girişindeki tüm kitleler için uygun olması gerekir.

Burada, birkaç en iyi uygulama bulabilirsiniz:

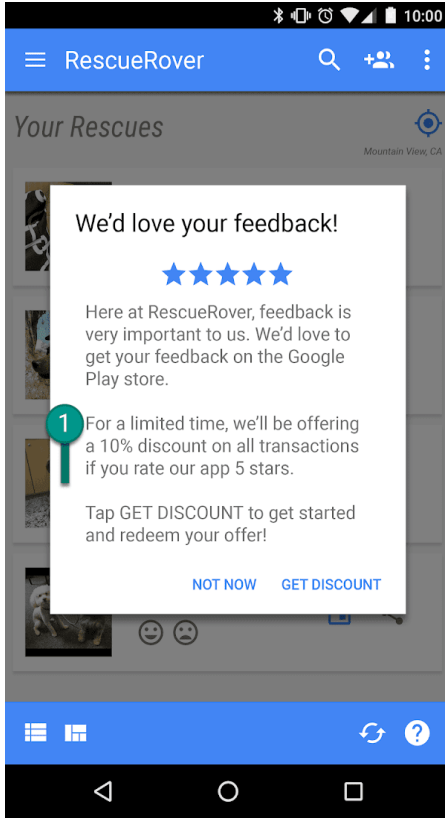
- Uygulamanızın en iyi yanlarını vurgulayın. Kullanıcıların uygulamanızı özel kılan unsurları anlamalarına yardımcı olmak için uygulamanız hakkında ilginç ve heyecan verici bilgiler paylaşın.
- Uygulama başlığınızın ve açıklamanızın, uygulamanızın işlevselliğini doğru bir şekilde açıkladığından emin olun.
- Tekrar eden ve ilgisiz anahtar kelimeler veya referanslar kullanmaktan kaçınınız.
- Uygulamanızın açıklamasını kısa ve öz tutun. Kısa açıklamalar, özellikle küçük ekranlı cihazlarda daha iyi kullanıcı deneyimi sunar. Aşırı uzun, ayrıntılı, yanlış biçimlendirilmiş veya tekrar eden açıklamalar bu politikanın ihlaliyle sonuçlanabilir.
- Girişinizin genel kitle için uygun olması gerektiğini unutmayın. Girişinizde uygunsuz metin, resim veya video kullanmaktan kaçınınız ve yukarıdaki kurallara uyun.

Kullanıcı Puanları, Yorumlar ve Yükleme

Geliştiriciler, Google Play'deki hiçbir uygulamanın yerleşimini hileli bir şekilde değiştirmeyi denememelidir. Bu kural, sahte veya teşvik yoluyla elde edilen yüklemeler, yorumlar ve puanlar gibi kural dışı yöntemlere başvurarak ürünün puanını yükseltme, yorumlarını şişirme veya yükleme sayılarını artırmayı içerir ancak bunlarla sınırlı değildir.

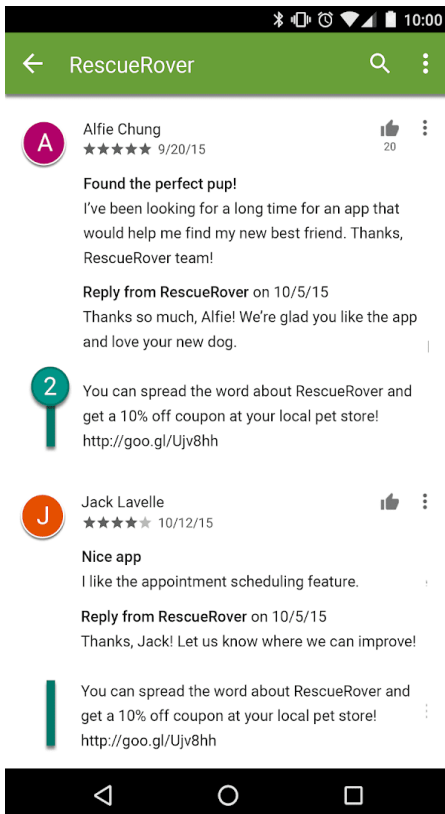
Yaygın görülen ihlallere ilişkin bazı örnekleri aşağıda bulabilirsiniz:

- Bir teşvik sunarken kullanıcılardan uygulamanız için oy vermelerini isteme:



① Bu bildirim, kullanıcılara yüksek oy vermeleri karşılığında indirim sunar.

- Uygulamanın Google Play'deki yerleşimini etkilemek için sürekli olarak puanlamalar gönderme.
- Satış ortakları, kuponlar, oyun kodları, e-posta adresleri veya web sitelerine ya da diğer uygulamalara bağlantılar da dahil olmak üzere, uygunsuz içerik barındıran yorumlar gönderme veya kullanıcıları bu tür yorumlar göndermeleri için teşvik etme:



② Bu yorum, bir kupon teklifi yaparak kullanıcıları RescueRover uygulamasını tanıtmaya teşvik eder.

Kullanıcı oyları ve yorumlar, uygulamanın kalitesini gösteren karşılaştırma ölçütleridir. Kullanıcılar, bu bilgilerin orijinal ve alakalı olmasına güvenir. Burada, kullanıcı yorumlarına yanıt verirken izleyebileceğiniz birkaç en iyi uygulama bulabilirsiniz:

- Yanıtınızın daha yüksek bir kullanıcı oyu istemek yerine kullanıcının yorumlarında açıkladığı sorunlara odaklı kaldığından emin olun.
- Destek adresi veya SSS sayfası gibi yararlı kaynaklar için referanslar ekleyin.

İçerik Derecelendirmeleri

Google Play'deki içerik derecelendirmeleri Uluslararası Yaş Derecelendirme Birliği (IARC) tarafından sağlanmakta olup geliştiricilerin yerel olarak alakalı içerik derecelendirmelerini kullanıcılara iletmesine yardımcı olmak üzere tasarlanmıştır. Bölgesel IARC yetkilileri, uygulamadaki içeriğin hangi yaşlara uygun olduğunu belirlemek için kullanılacak yönergeler sağlar. Google Play'de içerik derecelendirmesi olmayan uygulamalara izin verilmez.

İçerik derecelendirmeleri nasıl kullanılır?

İçerik derecelendirmeleri, tüketicileri (özellikle ebeveynleri) bir uygulamanın içindeki rahatsız edici olabilecek içerikler konusunda bilgilendirmek için kullanılır. Derecelendirmeler ayrıca yasal olarak gerektiğinde içeriğinizin belirli bölgelerde veya belirli kullanıcılar için filtrelenmesine ya da engellenmesine ve uygulamanızın, özel geliştirici programlarına uygun olup olmadığının belirlenmesine yardımcı olur.

İçerik derecelendirmeleri nasıl verilir?

İçerik derecelendirmesi almak için uygulamanızın içeriği hakkında [Play Console'da derecelendirme anketi](#) doldurmanız gerekir. Birden fazla derecelendirme kurumu, ankete verdiğiniz yanıtlara dayanarak uygulamanıza bir içerik derecelendirmesi verecektir. Uygulamanızın içeriğinin yanlış şekilde tanıtılması, uygulamanızın kaldırılmasına veya askıya alınmasına neden olabileceğinden içerik derecelendirme anketine doğru yanıtlar vermeniz önemlidir.

Uygulamanızın "Derecelendirilmemiş" olarak listelenmesini önlemek için Play Console'a gönderilen her yeni uygulamanın yanı sıra Google Play'de etkin olan tüm mevcut uygulamalar için içerik derecelendirme anketini doldurmanız gerekir.

Uygulamanızın içeriğinde veya özelliklerinde, derecelendirme anketine verilen yanıtları etkileyen değişiklikler yaparsanız Play Console'da yeni bir içerik derecelendirme anketi göndermeniz gerekir.

Farklı [derecelendirme kurumları](#) ve içerik derecelendirme anketini nasıl dolduracağınız hakkında daha fazla bilgi edinmek için [Yardım Merkezi](#)'ni ziyaret edin.

Derecelendirmeye itirazlar

Uygulamanıza verilen derecelendirmeyi kabul etmezseniz sertifika e-postanızdaki bağlantıyı kullanarak doğrudan IARC derecelendirme kurumuna itiraz edebilirsiniz.

Haberler

Kendisini Google Play'de "Haberler" uygulaması olarak tanımlayan bir uygulama aşağıdaki gereksinimlerin tümünü karşılamalıdır.

Kullanıcıların üyelik satın almasını gerektiren haber uygulamaları, satın alma işleminden önce kullanıcılara içerik önizlemesi sağlamalıdır.

Haber uygulamaları şunları YAPMALIDIR:

- uygulamanızda yayınlanan haberlerin resmi web sitesi, geçerli ve doğrulanabilir iletişim bilgileri ile her makalenin orijinal yayıncısı dahil ancak bunlarla sınırlı olmamak üzere, haberlerin yayıncısı ve katkıda bulunanlarla ilgili sahiplik bilgileri sağlamalı,
- haber yayıncısının geçerli iletişim bilgilerini içeren bir web sitesi veya uygulama içi sayfaya sahip olmalı.

Haber uygulamaları şunları YAPMAMALIDIR:

- önemli düzeyde yazım ve dil bilgisi hataları içermemeli,
- yalnızca statik içerik (ör. birkaç ay öncesine ait içerik) barındırmamalı,
- birincil amacı satış ortaklığı pazarlaması yapmak veya reklam geliri elde etmek olmamalı.

Farklı yayın kaynaklarından içerik toplayan haber toplama uygulamaları, uygulamadaki içeriğin yayın kaynağı konusunda şeffaf olmalı ve her kaynak, Haberler politikasının gereksinimlerini karşılamalıdır.

Spam ve Minimum İşlevsellik

Uygulamalarla ilgili asgari gereklilik, kullanıcılara basit derecede işlevsellik ve düzeyli bir kullanıcı deneyimi sunmaktır. Kilitlenen, işlevsel bir kullanıcı deneyimiyle tutarlı olmayan diğer davranışlar sergileyen veya yalnızca kullanıcılara ya da Google Play'e spam yapmaya yarayan uygulamalar, kataloğu anlamlı bir şekilde genişleten uygulamalar değildir.

Spam

Kullanıcılara istenmeyen mesajlar gönderen uygulamalar veya tekrar eden ya da düşük kalitede uygulamalar gibi kullanıcılara veya Google Play'e spam gönderen uygulamalara izin verilmez.

Mesaj Spam'ı

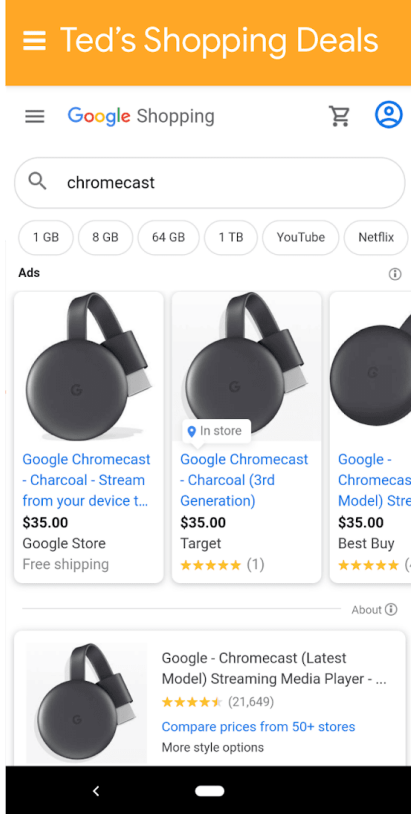
Kullanıcının adına SMS, e-posta veya başka iletiler gönderirken iletinin içeriğini ve gönderilecek alıcıları kullanıcının onaylamasına olanak sağlamayan uygulamalara izin verilmez.

Web Görüntülemeleri ve Satış Ortağı Spam'ı

Birincil amacı, bir web sitesine yönelik satış ortağı trafiğini artırmak veya web sitesi sahibinin ya da yöneticisinin izni olmadan bir web sitesinin web görünümünü sağlamak olan uygulamalara izin verilmez.

Yaygın görülen ihlallere ilişkin bazı örnekleri aşağıda bulabilirsiniz:

- Birincil amacı, kullanıcıların kaydolmasından veya bir web sitesindeki satın alma işlemlerinden kazanç elde etmek üzere ilgili web sitesine daha fazla trafik yönlendirmek olan uygulamalar.
- Birincil amacı, izin almadan bir web sitesinin web görünümünü sağlamak olan uygulamalar:



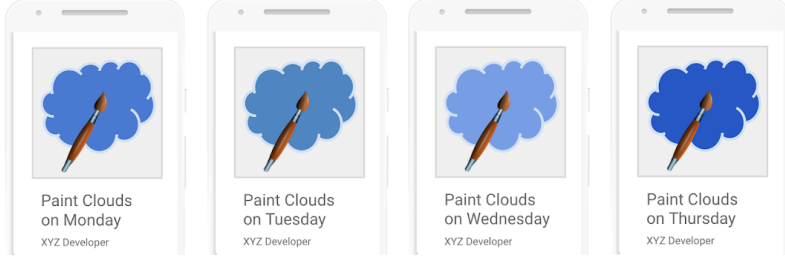
"Ted'in Alışveriş Fırsatları" adlı bu uygulama yalnızca Google Alışveriş'in web görünümünü sağlamaktadır.

Tekrar Eden İçerik

Tek işlevi Google Play'de halihazırda bulunan diğer uygulamalarla aynı deneyimi sunmak olan uygulamalara izin verilmez. Uygulamalar kullanıcılara benzersiz içerik veya hizmet sunarak değer katmalıdır.

Yaygın görülen ihlallere ilişkin bazı örnekleri aşağıda bulabilirsiniz:

- Orijinal içerik veya değer katmadan başka uygulamalardan içerik kopyalama
- Büyük oranda benzer içeriğe ve kullanıcı deneyimine sahip birden çok uygulama oluşturma. Bu uygulamalardan her birinin içerik hacmi düşükse geliştiriciler tüm içeriği bir araya getiren tek bir uygulama oluşturmaya çalışmalıdır.



Reklamlar için Üretilen

Asıl amacı reklam yayınlamak olan uygulamalara izin verilmez.

Yaygın görülen ihlallere ilişkin bazı örnekleri aşağıda bulabilirsiniz:

- Tıklama, kaydırma dahil ancak bunlarla sınırlı olmamak üzere her kullanıcı işleminden sonra geçiş reklamları yayınlanan uygulamalar

Minimum İşlevsellik

Uygulamanızın kararlı ve duyarlı bir kullanıcı deneyimi sunduğundan emin olun.

Yaygın görülen ihlallere ilişkin bazı örnekleri aşağıda bulabilirsiniz:

- Hiçbir şey yapmamak için tasarlanmış veya hiçbir işlevi olmayan uygulamalar

Bozuk İşlevsellik

Kilitlenen, zorla kapanan, donan veya başka anormal davranışlar gerçekleştiren uygulamalara izin verilmez.

Yaygın görülen ihlallere ilişkin bazı örnekleri aşağıda bulabilirsiniz:

- **Yüklenmeyen** uygulamalar
- Cihaza yüklenen ancak **belleğe yüklenemeyen** uygulamalar
- Belleğe yüklenen ancak **yanıt vermeyen** uygulamalar

Diğer Programlar

Diğer Android deneyimleri için tasarlanan ve Google Play aracılığıyla dağıtılan uygulamalar, bu Politika Merkezi'nin başka yerlerinde belirtilen içerik politikalarına uygunluğun yanı sıra, programa özel politika gereksinimlerine de tabi olabilir. Bu politikalarından herhangi birinin uygulamanız için geçerli olup olmadığını belirlemek amacıyla aşağıdaki listeyi incelediğinizden emin olun.

Android Hazır Uygulamalar

Android Hazır Uygulamalar ile amacımız en yüksek gizlilik ve güvenlik standartlarına uyarken aynı zamanda keyifli, akıcı kullanıcı deneyimleri oluşturmaktır. Politikalarımız bu hedefi destekleyecek şekilde tasarlanmıştır.

Google Play üzerinden Android Hazır Uygulamalar dağıtmayı seçen geliştiriciler, aşağıdaki politikaları ve diğer tüm [Google Play Geliştirici Program Politikaları](#)'na uymalıdır.

Kimlik

Giriş işlevselliği bulunan hazır uygulamalar için geliştiricilerin [Şifreler için Smart Lock](#)'u entegre etmesi gerekir.

Bağlantı Desteği

Android Hazır Uygulama geliştiricilerinin diğer uygulamalarla ilgili bağlantıları doğru şekilde desteklemeleri gerekir. Geliştiricinin hazır uygulaması veya yüklü uygulaması, hazır uygulamaya yönlendiren bağlantılar içeriyorsa geliştiricinin, örneğin bağlantıları [Web Görünümü](#) ile yakalamak yerine kullanıcıları söz konusu hazır uygulamaya göndermesi gerekir.

Teknik Özellikler

Geliştiriciler, Google tarafından sağlanan Android Hazır Uygulamalar teknik özelliklerine ve gereksinimlerine uymalıdır. [Herkese açık dokümanlarımızda](#) listenenler de dahil olmak üzere bu teknik özellikler ve gereksinimler zaman zaman değiştirilebilir.

Uygulama Yükleme Seçeneğini Sunma

Hazır uygulama, kullanıcıya yüklenebilir uygulamayı sunabilir ancak bu, hazır uygulamanın birincil amacı olmamalıdır. Yükleme seçeneğini sunarken geliştiriciler şunları yapmalıdır:

- Yükleme düğmesi için [Materyal Tasarım "uygulamayı yükle" simgesi](#) ve etiketini kullanmak.
- Hazır uygulamada en fazla 2-3 örtülü yükleme istemi bulundurmak.
- Kullanıcılara yükleme istemini sunmak için banner veya reklam benzeri başka bir tekniği kullanmamak.

Ek hazır uygulama ayrıntılarını ve kullanıcı deneyimi kurallarını [Kullanıcı Deneyimi için En İyi Uygulamalar](#)'da bulabilirsiniz.

Cihaz Durumunu Değiştirme

Hazır uygulamalar, kullanıcının cihazında etkisi hazır uygulama oturumundan daha uzun sürecek değişiklikler yapmamalıdır. Örneğin, hazır uygulamalar kullanıcının duvar kağıdını değiştiremez veya bir ana ekran widget'ı oluşturamaz.

Uygulama Görünürlüğü

Geliştiriciler, hazır uygulamaların kullanıcı tarafından görülebildiğinden yani hazır uygulama cihazında çalıştırılırken kullanıcının her zaman bunun farkında olduğundan emin olması gerekir.

Cihaz Tanımlayıcıları

Hazır uygulamaların, (1) hazır uygulama çalışması durduktan sonra kullanılmaya devam eden ve (2) kullanıcı tarafından sıfırlanamayan cihaz tanımlayıcılarına erişmesi yasaktır. İlgili örnekler aşağıdakileri kapsar, ancak bunlarla sınırlı değildir:

- Derleme Serisi
- Ağ iletişimi yongalarının Mac Adresleri
- IMEI, IMSI

Hazır uygulamalar, çalışma zamanı izni kullanılarak alınmışsa telefon numarasına erişebilir. Geliştirici, bu tanımlayıcıları veya başka araçları kullanarak parmak izini almaya çalışmamalıdır.

Ağ trafiği

Hazır uygulamanın içinden gerçekleştirilen ağ trafiği, HTTPS gibi bir TLS protokolü kullanılarak şifrlenmelidir.

Aileler

Google Play, geliştiricilerin tüm aile için yüksek kaliteli, yaşa uygun içerik sunmasına olanak veren zengin bir platform sağlar. Aileler için programına herhangi bir uygulama veya Google Play Store'da çocukları hedefleyen bir uygulama göndermeden önce, uygulamanızın çocuklar için uygunluğunu ve ilgili tüm yasalara uyumluluğunu sağlamaktan sorumlusunuz.

Aileler süreci hakkında bilgi edinin ve Başarılı Uygulama Akademisi'ndeki etkileşimli yapılacaklar listesini inceleyin.

Çocuklar ve Aileler için Uygulama Tasarlama

Ailelerin yaşamını zenginleştiren bir araç olarak teknolojinin kullanımı gittikçe artıyor ve ebeveynler çocuklarıyla paylaşabilecekleri güvenli, yüksek kalitede içerik arıyorlar. Uygulamalarınızı özel olarak çocuklar için tasarlıyor olabilirsiniz ya da uygulamanız çocukların ilgisini çekiyor olabilir. Google Play, uygulamanız aileler de dahil olmak üzere tüm kullanıcılar için güvenli mi, buna emin olmanıza yardım etmek istiyor.

"Çocuk" kelimesi farklı yerlerde ve değişik bağlamlarda farklı anlama gelebilir. Uygulamanız için geçerli olabilecek yükümlülükler ve/veya yaşa bağlı kısıtlamaları belirlemek için hukuk danışmanınızdan yardım almanız önemlidir. Uygulamanızın nasıl çalıştığını en iyi siz biliyorsunuz. Bu nedenle, Google Play'deki uygulamaların aileler için güvenli olmasını sağlama konusunda gereken yardımı sağlayacağınıza inanıyoruz.

Özel olarak çocuklar için tasarlanmış uygulamaların Aileler için programına dahil olması gerekmektedir. Uygulamanız hem çocukları hem de yaşça daha büyük kitleleri hedefliyorsa yine de Aileler için programına katılabilirsiniz. Aileler için

programına dahil olan tüm uygulamalar [Öğretmen Onaylı programı](#) için derecelendirilmeye uygun olur, ancak uygulamanızın Öğretmen Onaylı programına dahil edileceğini garanti edemeyiz. Aileler İçin programına katılmamaya karar verseniz bile aşağıdaki Google Play Aile Politikası şartlarının yanı sıra [Google Play Geliştirici Program Politikaları](#) ve [Geliştirici Dağıtım Sözleşmesi](#)'ne uymalısınız.

Play Console Şartları

[Hedef kitle ve içerik](#)

Uygulamanızı yayınlamadan önce, Google Play Console'un [Hedef Kitle ve İçerik](#) bölümünde belirtilen yaş grupları arasından seçim yaparak uygulamanızın hedef kitesini belirtmeniz gerekir. Google Play Console'da belirttiğiniz yaş gruplarından bağımsız olarak, uygulamanıza çocukları hedefleyen görsel malzemeler ve terminoloji eklerseniz bu durum Google'ın, açıkladığınız hedef kitleyle ilgili değerlendirmesini etkileyebilir. Google Play, uygulamanızla ilgili olarak açıkladığınız hedef kitlenin doğruluğunu belirlemek için uygulama bilgilerini inceleme hakkını saklı tutar.

Yalnızca yetişkinleri içeren bir hedef kitle seçmenize rağmen, uygulamanın hem çocukları hem de yetişkinleri hedeflemesi nedeniyle Google bu seçimin doğru olmadığını belirlerse uygulamanın çocukları hedeflemediğini açıkça belirtmek amacıyla bir uyarı etiketi görüntüleme seçeneğiniz olacaktır.

Uygulamanızın hedef kitlesi için birden fazla yaş grubunu yalnızca, uygulamayı seçilen yaş grubundaki kullanıcılar için tasarladıysanız ve uygulamanın bu kullanıcılara uygun olduğundan eminensiz seçmelisiniz. Örneğin, bebekler, 1-5 yaş arası çocuklar ve okul öncesi çocuklar için tasarlanmış uygulamalarda yalnızca "5 Yaş ve Altı" yaş grubu seçilmelidir. Uygulamanız belirli bir sınıfa giden öğrenciler tarafından kullanılmak üzere tasarlandıysa ilgili sınıfı en iyi yansıtan yaş grubunu seçin. Hem yetişkinleri hem de çocukları içeren yaş grubunu yalnızca, uygulamanızı gerçekten tüm yaşlar için tasarladıysanız seçmelisiniz.

Hedef Kitle ve İçerik Bölümü Güncellemeleri

Uygulamanızın Google Play Console'un Hedef Kitle ve İçerik bölümündeki bilgilerini istediğiniz zaman güncelleyebilirsiniz. Bu bilginin Google Play Store'a yansıtılabilmesi için önce bir [uygulama güncellemesi](#) yapılması gerekir. Bununla birlikte, Google Play Console'un bu bölümünde yapılan tüm değişiklikler, uygulama güncellemesi yüklenmeden önce bile politika uyumluluğu açısından incelenebilir.

Uygulamanızın hedef yaş kitlesini değiştirirseniz veya reklam ya da uygulama içi satın alma özellikleri kullanmaya başlarsanız, mağaza girişi sayfasındaki "Yenilikler" bölümünde veya uygulama içi bildirimlerle bu durumu mevcut kullanıcılarınıza bildirmenizi kesinlikle öneririz.

Play Console'da Yanlış Beyan

Play Console'da Hedef Kitle ve İçerik bölümündeki bilgiler de dahil olmak üzere uygulamanızla ilgili herhangi bir bilginin yanlış beyan edilmesi, uygulamanızın kaldırılmasına veya askıya alınmasına neden olabilir. Bu nedenle doğru bilgileri sağlamanız önemlidir.

Aile Politikası Şartları

Uygulamanızın hedef kitlelerinden biri çocuklarsa aşağıdaki şartlara uymanız gerekir. Bu şartlara uyulmaması durumunda uygulama kaldırılabilir veya askıya alınabilir.

- Uygulama içeriği:** Uygulamanızda çocukların erişebilecekleri içerik çocuklara uygun olmalıdır.
- Google Play Console Yanıtları:** Google Play Console'da uygulamanızla ilgili sorulara doğru yanıtlar vermeniz ve bu yanıtları uygulamanızda yapılacak herhangi bir değişikliği doğru yansıtacak şekilde güncellemeniz gerekir.
- Reklamlar:** Uygulamanız çocuklara veya yaşı bilinmeyen kullanıcılara reklam gösteriyorsa şunları yapmalısınız:
 - Bu kullanıcılara reklam göstermek için yalnızca [Google Play onaylı reklam SDK'larını](#) kullanmalısınız;
 - Bu kullanıcılara gösterilen reklamların ilgi alanına dayalı reklamcılık (internetdeki göz atma davranışlarına göre belirli özelliklere sahip bireysel kullanıcıları hedefleyen reklamlar) veya yeniden pazarlama (bir uygulama veya web sitesiyle önceki etkileşimine göre bireysel kullanıcıları hedefleyen reklamlar) içermemesini sağlamalısınız;
 - Bu kullanıcılara gösterilen reklamların, çocuklara uygun içerik sunduğundan emin olmalısınız;
 - Bu kullanıcılara gösterilen reklamların Aile reklam biçimiyle ilgili şartlara uyduğundan emin olmalısınız ve
 - Çocuklara reklam sunmayla ilgili geçerli tüm yasal düzenlemelere ve endüstri standartlarına uymalısınız.
- Veri Toplama:** Uygulamanızda çocuklardan [kişisel ve hassas bilgiler](#) toplanıyorsa bunu açıklamanız gerekir. Buna, uygulamanızın çağırıp kullandığı API'ler ve SDK'lar da dahildir. Kimlik doğrulama bilgileri, mikrofon ve kameraya ait sensör verileri, cihaz verileri, Android kimliği, reklam kullanım verileri ve reklam kimliği de dahil ancak bunlarla sınırlı olmayan bilgiler, çocuklardan toplanan hassas bilgiler kapsamına girer.
- API'ler ve SDK'lar:** Uygulamanızın API'leri ve SDK'ları doğru bir şekilde uyguladığından emin olmalısınız.
 - Yalnızca çocukları hedefleyen uygulamalar, çocuklara yönelik hizmetlerde kullanımı onaylanmamış API'leri veya SDK'ları içermemelidir. Buna Google ile Oturma Açma (veya Google Hesaplarıyla ilişkilendirilmiş verilere erişen diğer

Google API Hizmetleri), Google Play Oyunlar Hizmetlerinin yanı sıra kimlik doğrulama ve yetkilendirme amacıyla OAuth teknolojisini kullanan diğer tüm API hizmetleri dahildir.

- Hem çocukları hem de yaşça daha büyük kitleleri hedefleyen uygulamalar çocuklara yönelik hizmetlerde kullanımı onaylanmamış API'leri veya SDK'ları kullanmamalıdır. Bunun tek istisnası, söz konusu API'lerin ve SDK'ların [kısıtlamasız yaş seçme](#) işlevinin arkasında kullanılması veya çocuklardan veri toplanmasına (ör. Google ile Oturma Açma işlevini isteğe bağlı özellik olarak sunma) yol açmayan bir şekilde uygulanmasıdır. Hem çocukları hem de yaşça daha büyük kitleleri hedefleyen uygulamalar, kullanıcıların çocuklara yönelik hizmetlerde kullanımı onaylanmamış bir API veya SDK üzerinden oturum açmasını veya uygulama içeriğine erişmesini gerektirmemelidir.

6. **Gizlilik politikası:** Uygulamanızın mağaza girişi sayfasında gizlilik politikasının bağlantısına yer vermeniz gerekir. Uygulama, Play Store'da kullanılabilir olduğu sürece bu bağlantı her zaman bulunmalı ve diğer konuların yanı sıra uygulamanızın verileri nasıl toplayıp kullandığını açıklayan bir gizlilik politikasına bağlanmalıdır.

7. **Özel kısıtlamalar:**

- Uygulamanız Artırılmış Gerçeklik kullanıyorsa AR bölümü başlar başlamaz bir güvenlik uyarısı göstermeniz gerekir: Uyarı şunları içermelidir:
 - Ebeveyn gözetiminin önemi hakkında uygun bir mesaj
 - Gerçek dünyadaki fiziksel tehlikelerin farkında olmaya yönelik bir hatırlatma (ör. çevrenize dikkat edin)
- Uygulamanız, çocuklar tarafından kullanılması önerilmeyen bir cihazın (ör. Daydream, Oculus) kullanılmasını gerektirmemelidir.

8. **Yasalara Uygunluk:** Uygulamanızın çağırdığı veya kullandığı tüm API ve SDK'lar da dahil olmak üzere uygulamanızın [ABD'de Çocukların Çevrimiçi Gizliliğini Koruma Yasası \(COPPA\)](#), [AB'de Genel Veri Koruma Yönetmeliği \(GDPR\)](#) ve diğer tüm geçerli yasa ve yönetmeliklere uygunluğunu sağlamalısınız.

Yaygın görülen ihlallere ilişkin bazı örnekleri aşağıda bulabilirsiniz:

- Mağaza girişinde çocukların oynamaları için promosyon yapan, ancak içeriği yalnızca yetişkinlere uygun olan uygulamalar.
- Çocuklara yönelik uygulamalarda kullanımı yasaklayan hizmet şartlarına sahip API'leri uygulayan uygulamalar.
- Alkol, tütün ve kontrole tabi maddelerin kullanımını öven uygulamalar.
- Gerçek veya simülasyon kumar içeren uygulamalar.
- Çocuklar için uygun olmayan şiddet, kan veya şok edici içerik barındıran uygulamalar.
- Flört hizmetleri veya cinsellik ya da evlilikle ilgili öneriler sunan uygulamalar.
- Google Play'in [Geliştirici Program politikalarını](#) ihlal eden içerik sunan web sitelerinin bağlantılarını içeren uygulamalar.
- Yetişkinlere yönelik reklamları (ör. şiddet barındıran içerik, cinsel içerik, kumar içeriği) çocuklara gösteren uygulamalar. Google Play'in çocuklara yönelik reklamcılık, uygulama içi satın alma ve ticari içerik politikaları hakkında daha fazla bilgi edinmek için [Aile Reklamları ve Para Kazanma politikalarına](#) bakabilirsiniz.

Aileler İçin Programı

Özel olarak çocuklar için tasarlanmış uygulamaların Aileler İçin programına dahil olması gerekmektedir. Uygulamanız çocuklar ve aileler dahil herkes için tasarlandıysa siz de programa katılmak için başvurabilirsiniz.

Uygulamanız programa kabul edilmeden önce tüm Aile Politikası gereksinimlerine, Aileler için programının uygunluk koşullarına ve [Google Play Geliştirici Program Politikaları](#) ile [Geliştirici Dağıtım Sözleşmesi](#)'nde belirtilen gereksinimlere uymalıdır.

Uygulamanızı programa dahil edilmek üzere gönderme süreciyle ilgili daha fazla bilgiyi [burada](#) bulabilirsiniz.

Programa Uygunluk

Aileler İçin programına katılan tüm uygulamaların hem kendi hem de reklam içeriğinin çocuklarla ilgili ve çocuklara uygun olması ve aşağıdaki tüm koşulları karşılaması gerekir. Aileler için programına kabul edilen uygulamalar tüm program şartlarına uymaya devam etmelidir. Google Play, Aileler için programına uygun olmadığı belirlenen uygulamaları reddedebilir, kaldırabilir veya askıya alabilir.

Aileler İçin Şartları

- Uygulamaların ESRB Herkes veya 10 Yaş Üzerindeki Herkes ya da eşdeğeri bir derecelendirmeye sahip olması gerekir.
- Google Play Console'daki İçerik Derecelendirme Anketi'nde uygulamanın etkileşimli öğelerinin, aşağıdaki işlevlere sahip olup olmadığını doğru olarak beyan etmeniz gerekir:
 - Kullanıcıların etkileşim kurabilmesi veya bilgi alışverişinde bulunabilmesi;
 - kullanıcı tarafından sunulan kişisel bilgilerin üçüncü taraflarla paylaşılması ve
 - kullanıcının fiziksel konumunun diğer kullanıcılarla paylaşılması.
- Uygulamanız [Android Speech API'sini](#) kullanıyorsa uygulamanın RecognizerIntent.EXTRA_CALLING_PACKAGE seçeneği packageName değerine ayarlanmalıdır.

4. Uygulamalar yalnızca [Google Play onaylı reklam SDK'larını](#) kullanmalıdır.
5. Çocuklar için tasarlanmış uygulamalar konum izni isteğinde bulunamaz.
6. Bluetooth kullanımı isteğinde bulunan uygulamalar [Companion Device Manager'ı \(CDM\)](#) kullanmalıdır (uygulamanız yalnızca CDM ile uyumlu olmayan cihaz İşletim Sistemi (OS) sürümlerini hedeflemiyorsa).

Programa uygun olmayan genel uygulamalara bazı örnekler:

- ESRB Herkes olarak derecelendirilmesine rağmen kumarla ilgili reklamlar içeren uygulamalar
- Ebeveynler veya bakıcılar için uygulamalar (ör. emzirme takip programı, gelişim rehberi)
- Yalnızca ebeveynler veya bakıcıların kullanımı için hazırlanmış ebeveyn rehberleri veya cihaz yönetim uygulamaları
- Çocuklar için uygun olmayan bir uygulama simgesi veya başlatıcı simgesi kullanan uygulamalar

Kategoriler

Aileler için programına katılmanız kabul edilirse uygulamanızı tanımlayan ikinci bir Aileye özel kategori seçebilirsiniz. Aileler için programına katılan uygulamaların kullanabileceği kategoriler şunlardır:

Aksiyon ve Macera: Aksiyona yönelik uygulamalar/oyunlardır. Bunlar, basit yarış oyunlarından masal temalı maceralara ve heyecan yaratmak için tasarlanmış diğer uygulama ve oyunlara kadar her şeyi içerir.

Zeka Oyunları: Kullanıcının düşünmesini sağlayan oyunlardır. Bunların arasında bulmacalar, eşleştirme oyunları, testlerin yanı sıra hafızayı, zekayı ve mantığı zorlayacak oyunlar bulunur.

Yaratıcılık: Yaratıcılığı teşvik eden uygulama ve oyunlardır. Bunların arasında çizim uygulamaları, boyama uygulamaları, kodlama uygulamaları ve bir şeyler oluşturabileceğiniz diğer uygulama ve oyunlar bulunur.

Eğitim: Öğrenmeyi desteklemek için eğitim uzmanlarının (ör. öğretmenler, eğitmenler, araştırmacılar) sağladığı bilgilerle tasarlanmış uygulama ve oyunlardır. Bunların arasında akademik, sosyal-duygusal, fiziksel ve yaratıcı öğrenmenin yanı sıra yaşamla ilgili temel beceriler, eleştirel düşünme ve sorun çözme gibi öğrenmeyle ilgili konular yer alır.

Müzik ve Video: Müzikal veya video bileşeni içeren uygulama ve oyunlardır. Bunların arasında müzik aleti simülasyon uygulamalarından video ve müzik içeriği sağlayan uygulamalara kadar her şey bulunur.

Rol Yapma: Kullanıcıların bir role bürünebildiği uygulama ve oyunlardır. Örneğin, şef aşçı, bakıcı, prens/prenses, itfaiyeci, polis memuru veya hayali karakter rolü yapma.

Reklamlar ve Para Kazanma

Aşağıdaki politikalar, Aile Politikası'nın ve/veya Aileler için programının Şartlarına tabi olan uygulamaların kullanıcılarına sunulan tüm reklamlar (hem uygulamalarınız için hem de üçüncü taraf uygulamalar için olanlar dahil), uygulama içi satın alma teklifleri veya her tür ticari içerik (ücretli ürün yerleşimi gibi) için geçerlidir. Bu uygulamalardaki uygulama içi satın alma işlemleri ve ticari içerik için sunulan tüm reklamlar (ilgili tüm öz denetim veya endüstri yönergeleri dahil olmak üzere) tüm geçerli yasalara ve yönetmeliklere uymalıdır.

Google Play aşırı agresif ticari taktikler kullanan uygulamaları reddetme, kaldırma veya askıya alma hakkını saklı tutar.

Reklam biçimi şartları

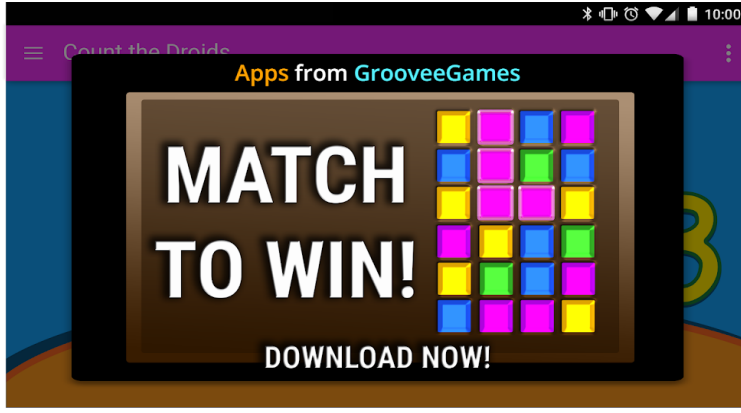
Uygulama içi satın almalar için reklamlar ve teklifler, aldatıcı içeriğe sahip veya çocuk kullanıcıların yanlışlıkla tıklamasına sebep olacak şekilde tasarlanmış olmamalıdır. Aşağıdakiler yasaklanmıştır:

- Ekranın tamamını kaplayan veya normal kullanımı aksatan ve reklamı kapatmak için açık bir yol sağlamayan reklamlar da dahil olmak üzere kullanımı engelleyen reklamlar (ör. [Reklam duvarları](#))
- Normal uygulama kullanımı veya oyun oynamayı engelleyen ve 5 saniye sonra kapatılamayan reklamlar. Normal uygulama kullanımı veya oyun oynamayı engellemeyen reklamlar 5 saniyeden uzun süre devam edebilir (ör. entegre reklamlar içeren video içeriği).
- Uygulama içi satın alma için geçiş reklamları veya tekliflerin, uygulama başladıktan hemen sonra görüntülenmesi
- Bir sayfada birden fazla reklam yerleşimi (ör. bir yerleşimde birden çok teklif gösteren veya birden fazla banner ya da video reklam gösteren banner reklamlara izin verilmez).
- Uygulama içeriğinizden farkı açıkça belli olmayan uygulama içi satın almalar için reklamlar ve teklifler
- Reklamların görüntülenmesini veya uygulama içi satın alma işlemlerinin gerçekleştirilmesini teşvik etmek için sarsıcı veya duygusal açıdan manipülatif taktiklerin kullanılması
- Uygulama içi satın alma işlemleri gerçekleştirmek için sanal oyun paraları ile gerçek para arasında ayırım sağlamama

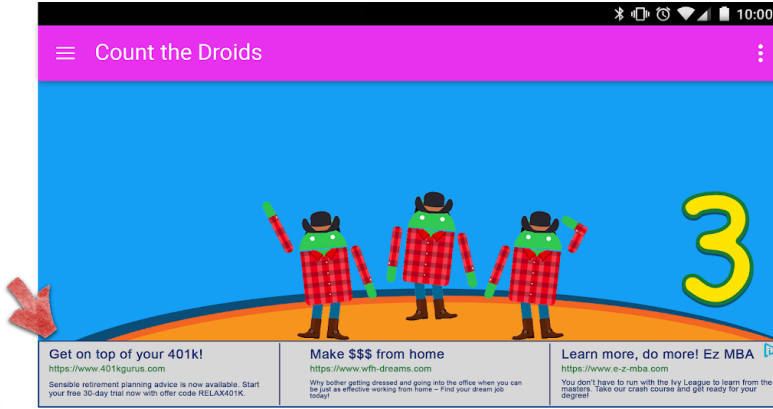
Sık karşılaşılan reklam biçimi ihlalleriyle ilgili bazı örnekler

- Kullanıcı kapatmaya çalışırken kullanıcının parmağından uzaklaşan reklamlar

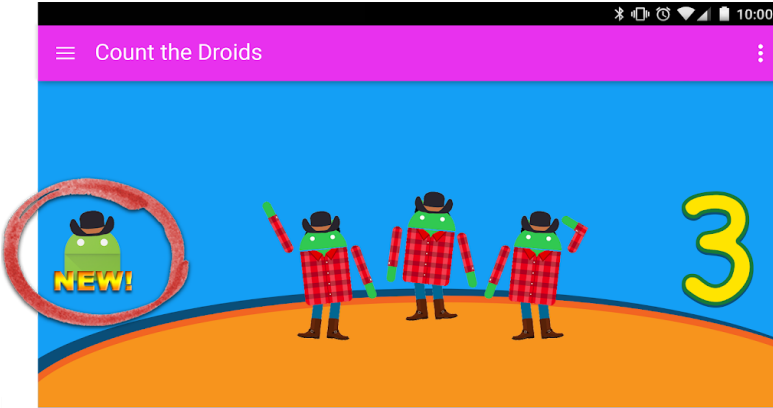
- Aşağıdaki örnekte gösterildiği gibi, ekranın büyük kısmını veya cihaz ekranını kaplayan ve kullanıcıya kapatmak için açıkla anlaşılar bir yöntem sunmayan reklamlar:



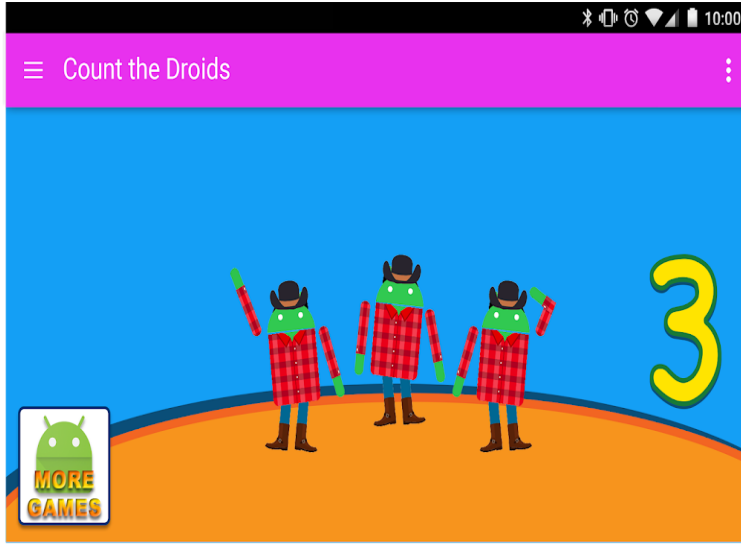
- Birden fazla teklif gösteren, aşağıdaki gibi banner reklamlar:



- Kullanıcının uygulama içeriğiyle karıştırılabileceği aşağıdaki gibi reklamlar:



- Diğer Google Play mağaza girişlerini tanıtan, ancak uygulama içeriğinden ayırt edilemeyen aşağıdaki örnekte gösterildiği gibi düğmeler veya reklamlar:



Çocuklara gösterilmemesi gereken bazı uygunsuz reklam içeriği örneklerini aşağıda bulabilirsiniz.

- **Uygunsuz Medya İçeriği:** Çocuklar için uygun olmayan TV programları, filmler, müzik albümleri veya diğer medya ürünlerinin reklamları.
- **Uygunsuz Video Oyunları ve İndirilebilir Yazılımlar:** Çocuklar için uygun olmayan indirilebilir yazılımlar ve elektronik video oyunları için reklamlar.
- **Kontrol Tabi ve Zararlı Maddeler:** Alkol, tütün, kontrole tabi maddeler veya diğer zararlı maddelere yönelik reklamlar.
- **Kumar:** Girişi ücretsiz olsa dahi kumar simülasyonu, yarışma ve çekiliş promosyonlarıyla ilgili reklamlar.
- **Yetişkinlere Yönelik ve Müstehcen İçerik:** Cinsellik barındıran, müstehcen ve erişkinlere uygun içeriğe sahip reklamlar.
- **Arkadaşlık veya İlişkiler:** Arkadaşlık amaçlı veya yetişkinlerin ilişki kurmalarına yönelik sitelerin reklamları.
- **Şiddet Barındıran İçerik:** Çocuklara uygun olmayan şiddet ve vahşet içerikli reklamlar.

Reklam SDK'ları

Uygulamanızda reklam yayınlıyorsanız ve hedef kitleniz yalnızca çocukları içeriyorsa [Google Play onaylı reklam SDK'larını](#) kullanmanız gerekir. Uygulamanızın hedef kitlesi hem çocukları hem de yaşça daha büyük kullanıcıları içeriyorsa [kısıtlamasız yaş seçme ekranı](#) gibi yaş filtreleme önlemleri uygulayarak çocuklara gösterilen reklamların yalnızca Google Play onaylı reklam SDK'larından geldiğinden emin olmanız gerekir. Aileler için programında yer alan uygulamaların yalnızca içerik üretici onaylı reklam SDK'larını kullanması zorunludur.

Bu şartlarla ilgili daha fazla bilgi edinmek ve onaylı reklam SDK'larının güncel listesini görmek için [Aile Reklam Programı politikası](#) sayfasına bakabilirsiniz.

AdMob kullanıyorsanız ürünleriyle ilgili daha fazla ayrıntı için [AdMob Yardım Merkezi](#)'ne bakın.

Uygulamanızın reklamlar, uygulama içi satın alma işlemleri ve ticari içerikle ilgili tüm şartları karşılamasını sağlamak sizin sorumluluğunuzdur. İçerik politikaları ve reklam uygulamalarıyla ilgili daha fazla bilgi edinmek için reklam SDK'sı sağlayıcınızla iletişime geçin.

Uygulama içi satın alma

Google Play, Aileler için programında yer alan uygulamalardaki uygulama içi satın alma işlemlerinden önce tüm kullanıcıların kimliklerini yeniden doğrulayacaktır. Bu önlem, satın alma işlemlerini çocukların değil, finansal olarak sorumlu kişilerin onayladığından emin olmak içindir.

Yaptırım

Politika ihlalden kaçınmak, her zaman için politika ihlalden sonra durumu düzeltmeye çalışmaktan daha iyidir. Ancak ihlal oluştuğunda, geliştiricilerin, uygulamalarını politikayla nasıl uyumlu hale getirebileceklerini anladıklarından emin olmak için çalışırız. [Herhangi bir ihlal görürseniz](#) veya [bir ihlali yönetme](#) konusunda sorunuz olursa lütfen bize bildirin.

Politika Kapsamı

Politikalarımız, uygulamanızın görüntülediği veya bağlantı verdiği tüm içerikleri kapsar. Bu, kullanıcılara gösterilen reklamları ve uygulamanın barındırdığı veya bağlantı verdiği, kullanıcılar tarafından oluşturulmuş içerikleri kapsar. Ayrıca,

Google Play'de herkese açık olarak görüntülenen, geliştirici adınız ve geliştirici web sitenize ilişkin listelenen açılış sayfası dahil geliştirici hesabınıza ait içerikler için de geçerlidir.

Kullanıcıların cihazlarına başka uygulamalar yüklemesine izin veren uygulamalara izin verilmez. Üçüncü tarafların sağladığı özellikler ve deneyimler de dahil olmak üzere, yüklenmeden başka uygulamalara, oyunlara veya yazılımlara erişim sağlayan uygulamalar, erişim sağladıkları içeriğin tamamının tüm [Google Play politikalarına](#) uygun olmasını sağlamalıdır ve bu uygulamalar, ek politika incelemelerine tabi tutulabilir.

Bu politikalarda kullanılan tanımlanmış terimler, [Geliştirici Dağıtım Sözleşmesi](#)'ndeki (GDS) terimlerle aynı anlama gelmektedir. Uygulamanızın içeriği bu politikalara ve GDS'ye uymalı, ayrıca [İçerik Derecelendirme Yönergelerimize](#) uygun olarak derecelendirilmelidir.

Kullanıcıların Google Play ekosistemine güvenini sarsan uygulamalara veya uygulama içeriklerine izin verilmez. Google Play'deki uygulamaların dahil edilip edilmeyeceğini değerlendirirken, sistemli bir şekilde zararlı davranışta bulunma veya kötüye kullanımla ilgili yüksek risk dahil, ancak bunlarla sınırlı olmamak üzere pek çok etkeni dikkate alırız. Uygulamaya ve geliştiriciye özel şikayetler, haber bildirimi, önceki ihlal geçmişi, kullanıcı geri bildirimi ve popüler markaların, karakterlerin ve diğer öğelerin kullanımı dahil ancak bunlarla sınırlı olmamak üzere kötüye kullanım riskini tanımlarız.

Google Play Protect nasıl çalışır?

Google Play Protect, uygulamaları yüklediğinizde kontrol eder. Ayrıca, cihazınızda periyodik olarak taramalar da gerçekleştirir. Zararlı olabilecek bir uygulama bulursa şunları yapabilir:

- Size bildirim gönderir. Uygulamayı kaldırmak için bildirim ve ardından [Yüklemeyi Kaldır](#)'a dokununuz.
- Siz yüklemeyi kaldırana kadar uygulamayı devre dışı bırakır.
- Uygulamayı otomatik olarak kaldırır. Çoğu durumda, zararlı bir uygulama tespit edilirse uygulamanın kaldırıldığını belirten bir bildirim alırsınız.

Kötü amaçlı yazılım korumasının işleyiş şekli

Kötü amaçlı üçüncü taraf yazılımlara, URL'lere ve diğer güvenlik sorunlarına karşı sizi korumak için Google, aşağıdakiler hakkında bilgi alabilir:

- Cihazınızın ağ bağlantıları
- Zararlı olabilecek URL'ler
- İşletim sisteminiz ve Google Play veya diğer kaynaklar üzerinden cihazınıza yüklenmiş uygulamalar.

Google'dan, bir uygulamanın veya URL'nin güvenli olmayabileceği konusunda uyarı alabilirsiniz. Cihazlar, veriler veya kullanıcılar için zararlı olduğu biliniyorsa uygulama veya URL, Google tarafından kaldırılabilir ya da yüklenmesi engellenebilir.

Bu korumalardan bazılarını cihaz ayaralarınızdan devre dışı bırakabilirsiniz. Ancak Google Play üzerinden yüklenen uygulamalarla ilgili olarak Google'a bilgi aktarılmaya ve başka kaynaklardan cihazınıza yüklenen uygulamaların Google'a herhangi bir bilgi gönderilmeden güvenlik sorunları açısından kontrol edilmesine devam edilebilir.

Gizlilik uyarılarının işleyiş şekli

Google Play Protect, bir uygulama kişisel bilgilerinize erişebileceği için Google Play Store'dan kaldırılırsa sizi uyarır. Böyle bir durumda uygulamanın yüklemesini kaldırma seçeneğine sahip olursunuz.

Yaptırım Süreci

Uygulamanız politikalarımızdan herhangi birini ihlal ediyorsa aşağıda belirtildiği gibi gereken işlemi yaparız. Ayrıca size e-posta göndererek yaptığımız işlem hakkında bilgi verir ve hatalı işlem yaptığımızı düşünüyorsanız nasıl itirazda bulunacağınızı anlatırız.

Uygulama kaldırma işlemi veya yönetimle ilgili bildirimlerin, uygulamanızda veya daha geniş bağlamda uygulama kataloğunuzda bulunan politika ihlallerinin hepsini belirtmeyebileceğini lütfen unutmayın. Politika sorunlarını giderme ve uygulamanın geri kalanının politikalarla tam olarak uyumlu olması için gereken ekstra özeni gösterme sorumluluğu geliştiricilere aittir. Tüm uygulamalarınızda politika ihlallerinin giderilmemesi ek yaptırımlara neden olabilir.

Bu politikalar ya da [Geliştirici Dağıtım Sözleşmesi](#) (GDS) ile ilgili tekrar eden veya ciddi düzeydeki ihlaller (kötü amaçlı yazılım, sahtekarlık ve kullanıcılara ya da cihazlara zarar verebilecek uygulamalar), bireysel hesabın veya ilgili Google Play Geliştirici hesaplarının feshedilmesiyle sonuçlanır.

Yaptırım İşlemleri

Farklı yaptırım işlemleri uygulamanızı farklı şekillerde etkileyebilir. Aşağıdaki bölümde, Google Play'in gerçekleştirebileceği çeşitli işlemler ve bunların uygulamanız ve/veya Google Play Geliştirici hesabınız üzerindeki etkisi açıklanmaktadır. Bu bilgilerle ilgili açıklamayı [bu videoda](#) da bulabilirsiniz.

Reddetme

- İnceleme için gönderilen yeni bir uygulama veya uygulama güncellemesi Google Play'de kullanıma sunulmaz.
- Mevcut bir uygulamada yapılan bir güncelleme reddedildiyse güncellemenin önce yayınlanan uygulama sürümü Google Play'de kullanıma sunulmaya devam eder.
- Reddetme işlemleri, reddedilen bir uygulamanın mevcut kullanıcı yüklemelerine, istatistiklerine ve puanlarına erişiminizi etkilemez.
- Reddetme işlemleri Google Play Geliştirici hesabınızın durumunu etkilemez.

Not: Tüm politika ihlallerini giderene kadar reddedilen bir uygulamayı yeniden göndermeyi denemeyin.

Kaldırma

- Uygulama önceki sürümleriyle birlikte Google Play'den kaldırılır ve artık kullanıcılar tarafından indirilemez.
- Uygulama kaldırıldığı için kullanıcılar uygulamanın Mağaza girişini, kullanıcı yüklemelerini, istatistiklerini ve puanlarını göremez. Kaldırılan uygulama için politikaya uygun bir güncelleme gönderdiğinizde bu bilgiler geri yüklenir.
- Kullanıcılar, politikaya uygun bir sürüm Google Play tarafından onaylanana kadar uygulama içi satın alma işlemi gerçekleştiremeyebilir veya uygulama içi faturalandırma özelliklerini kullanamayabilir.
- Kaldırma işlemleri Google Play Geliştirici hesabınızın durumunu hemen etkilemez, ancak birden fazla kaldırma işlemi hesabın askıya alınmasına neden olabilir.

Not: Tüm politika ihlallerini giderene kadar kaldırılan bir uygulamayı yeniden yayınlamayı denemeyin.

Askıya Alma

- Uygulama önceki sürümleriyle birlikte Google Play'den kaldırılır ve artık kullanıcılar tarafından indirilemez.
- Çok dikkat çekici düzeyde veya birden çok kez tekrarlayan politika ihlalleri askıya alınmayla sonuçlanabilir. Aynı şekilde uygulamaların birden fazla kez reddedilmesi veya kaldırılması da askıya alınmaya yol açabilir.
- Uygulama askıya alındığı için kullanıcılar uygulamanın Mağaza girişini, mevcut kullanıcı yüklemelerini, istatistiklerini ve puanlarını göremez. Kaldırılan uygulama için politikaya uygun bir güncelleme gönderdiğinizde bu bilgiler geri yüklenir.
- Askıya alınmış bir uygulamanın APK'sını veya uygulama paketini artık kullanamazsınız.
- Kullanıcılar, politikaya uygun bir sürüm Google Play tarafından onaylanana kadar uygulama içi satın alma işlemi gerçekleştiremez veya uygulama içi faturalandırma özelliklerini kullanamaz.
- Askıya alma işlemleri, Google Play Geliştirici hesabınızın iyi durumunu olumsuz etkileyen ihtarlar olarak sayılır. Birden fazla ihtar, bireysel ve ilgili Google Play Geliştirici hesaplarının feshedilmesine neden olabilir.

Not: Google Play bunu yapabileceğinizi açıklamadığı sürece askıya alınmış bir uygulamayı yeniden yayınlamayı denemeyin.

Sınırlı Görünürlük

- Uygulamanızın Google Play'deki bulunabilirliği kısıtlanır. Uygulamanız Google Play'de kullanıma sunulmaya devam eder ve kullanıcılar, Play mağaza girişine doğrudan bağlantıyla uygulamanıza erişebilir.
- Uygulamanızın Sınırlı Görünürlük durumuna geçirilmesi, Google Play Geliştirici hesabınızın durumunu etkilemez.
- Uygulamanızın Sınırlı Görünürlük durumuna geçirilmesi, kullanıcıların uygulamanın mevcut Mağaza girişini, kullanıcı yüklemelerini, istatistiklerini ve puanlarını görmesini etkilemez.

Hesabın Feshi

- Geliştirici hesabınız feshedildiğinde kataloğunuzdaki tüm uygulamalar Google Play'den kaldırılır ve artık yeni uygulama yayınlamazsınız. Bu, ilgili tüm Google Play geliştirici hesaplarının da kalıcı olarak askıya alınacağı anlamına gelir.
- Birden fazla kez tekrarlayan veya çok ciddi düzeydeki ihlaller Play Console hesabınızın feshedilmesine de yol açabilir.
- Feshedilen hesaptaki uygulamalar kaldırıldığından kullanıcılar uygulamaların Mağaza girişini, mevcut kullanıcı yüklemelerini, istatistiklerini ve puanlarını göremez.

Not: Açmaya çalışacağınız tüm yeni hesaplar da geliştirici kayıt ücreti geri ödenmeden feshedileceğinden diğer hesaplarınızdan biri feshedildiğinde lütfen yeni bir Play Console hesabına kaydolmaya çalışmayın.

Politika İhlallerini Yönetme ve Bildirme

How to handle a policy violation on Go...



Yaptırım İşlemine İtiraz Etme

Uygulamaları, bir hata yapıldıysa ve uygulamanızın Google Play Program Politikaları'nı ve Geliştirici Dağıtım Sözleşmesi'ni ihlal etmediği belirlenirse yeniden etkinleştiririz. Politikaları dikkatli bir şekilde incelediyseniz ve kararımızın hatalı olabileceğini düşünüyorsanız kararımıza itiraz etmek için yaptırım e-postası bildiriminde belirtilen talimatları uygulayabilirsiniz.

Ek Kaynaklar

Bir yaptırım işlemi veya bir kullanıcının puanı/yorumu hakkında daha fazla bilgiye ihtiyacınız varsa aşağıdaki kaynaklardan bazılarına başvurabilir ya da [Google Play Yardım Merkezi](#)'nden bize ulaşabilirsiniz. Ancak, size yasal danışmanlık sağlayamayız. Yasal danışmanlığa ihtiyacınız varsa lütfen hukuk danışmanınıza başvurun.

- [Uygulama doğrulama ve itirazlar](#)
- [Politika ihlali bildirme](#)
- [Bir hesabın feshi veya uygulamanın kaldırılmasıyla ilgili olarak Google Play ile iletişime geçme](#)
- [Kayda değer uyarılar](#)
- [Uygunsuz uygulamaları ve yorumları bildirme](#)
- [Uygulamam Google Play'den kaldırıldı](#)
- [Google Play geliştirici hesabı fesihlerini anlama](#)

Daha fazla yardıma mı ihtiyacınız var?

Bir sonraki adımları deneyin:

Bize ulaşın

Bize daha fazla bilgi verin, size yardımcı olalım