

Geliştirici Program Politikası

(Aksi belirtilmediği sürece 5 Mart 2025'ten 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

Çocukların istismar veya taciz edilmesini kolaylaştıran içeriklerin kullanıcılar tarafından oluşturulmasını, yüklenmesini ya da dağıtılmasını engellemeyen uygulamalar Google Play'den anında kaldırılır. Bu içeriklere, çocukların cinsel istismarı nitelikli materyallerin tümü dahildir. Google ürünlerinde, bir çocuğu istismar ediyor olabilecek içerikleri bildirmek için [Kötüye kullanım bildir](#) 'i tıklayın. İnternette başka bir yerde bu tür bir içerikle karşılaşırsanız lütfen doğrudan [ülkenizdeki ilgili kuruma](#) iletişime geçin.

Çocukları tehlikeye atan uygulamaların kullanımını yasaklarız. Bu yönerge, çocuklara karşı aşağıdaki gibi yıkıcı ve taciz edici davranışları teşvik eden uygulamaların kullanımını içerir ancak bunlarla sınırlı değildir:

- Çocuklarla uygunsuz etkileşimler (ör. elle taciz veya okşama)
- Cinsel temas amacıyla çocukları kandırmak için yapılan planlı eylemler (ör. bir çocukla internet üzerinden veya gerçek hayatta cinsel temas kurmak ve/veya çocuğa cinsel içerikli resim göndermek ya da almak için çocukla internette arkadaş olmak)
- Küçüğün cinselleştirilmesi (örneğin, çocukların cinsel istismarını tasvir veya teşvik eden ya da destekleyen veya çocuklara, çocukların cinsel istismarına yol açabilecek şekilde yer verilen görüntüler)
- Cinsel şantaj (ör. bir çocuğun mahrem görüntülerine erişilerek veya erişildiği iddia edilerek çocuğun tehdit edilmesi veya çocuğa şantaj yapılması)
- Çocuk ticareti (ör. bir çocuğun ticari cinsel istismar için pazarlanması veya buna teşvik edilmesi)

Çocukların cinsel istismarı nitelikli materyaller barındıran içeriklerden haberdar olmamız halinde Ulusal Kayıp ve Cinsel İstismara Uğrayan Çocuklar Merkezi'ne raporlama gibi gerekli işlemleri yaparız. Bir çocuğun taciz, istismar veya insan ticaretine maruz kalma tehlikesi altında olduğunu ya da bu eylemlere maruz kaldığını düşünüyorsanız lütfen yerel kolluk kuvvetinize başvurun ve [burada](#) listelenen çocuk güvenliği kuruluşlarından biriyle iletişime geçin.

Ayrıca, aşağıdakiler de dahil ancak bunlarla sınırlı olmamak üzere, çocuklara hitap etmesine rağmen yetişkinlere uygun temalar içeren uygulamalara izin verilmez:

- Aşırı şiddet ve kan içeren uygulamalar
- Zararlı ve tehlikeli etkinlikleri tasvir veya teşvik eden uygulamalar

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.

Çocuk Güvenliği Standartları Politikası

Google Play, sosyal medya ve arkadaşlık uygulamalarının Çocuk Güvenliği Standartları Politikamıza uymasını zorunlu tutar.

Bu uygulamaların aşağıdaki şartlara uyması gerekir:

- **Yayınlanmış Standartlara Sahip Olma:** Uygulamanız; Hizmet Şartları, Topluluk Kuralları veya herkese açık diğer kullanıcı politikası dokümanları gibi herkesin erişebileceği standartlarda çocuğun cinsel istismarı ve çocuk istismarını (CSAE) açık bir şekilde yasaklamalıdır.
- **Kullanıcı Geri Bildirimi için Uygulama İçi Yöntem Sağlama:** Uygulamanızda kullanıcıların geri bildirimde bulunma, endişelerini iletme veya bildirim göndermeleri için yöntem sağladığınıza dair içerik üretici onayı sunmalısınız.
- **Çocukların Cinsel İstismarı Nitelikli Materyalleri (CSAM) Ele Alma:** Uygulamanızın, tespit edildikten sonra CSAM'yi kaldırma dahil ancak bununla sınırlı olmamak üzere yayınlanan standartlarınız ve ilgili yasalar doğrultusunda uygun işlemleri gerçekleştirdiğine dair içerik üretici onayı sunmalısınız.
- **Çocukların Güvenliğiyle İlgili Yasalara Uyma:** Uygulamanızın, mevcut olduğu onaylanan CSAM'nin [ABD Ulusal Kayıp ve İstismara Uğramış Çocuklar Merkezi](#) veya [bölgenizdeki ilgili kuruma](#) bildirilebileceği bir süreçte sahip olması dahil ancak bununla sınırlı olmamak üzere çocukların güvenliğiyle ilgili geçerli yasalara ve yönetmeliklere uygun olduğuna dair içerik üretici onayı sunmanız gerekir.
- **Çocukların Güvenliği Konusunda İlgili Kişinin Bilgilerini Sağlama:** Uygulamanızda veya platformunuzda bulunan CSAE içerikleri hakkında Google Play'den olası bildirimleri almak için uygulamanızın, belirlenmiş ilgili kişinin bilgilerini sağlaması gerekir. Bu temsilcinin, yaptırım ve inceleme süreçleriniz hakkında söz hakkı olan, gerekirse de işlem yapabilecek bir konumda olması gerekir.

Bu şartlar ve şartlara nasıl uyacağınız hakkında daha fazla bilgi edinmek için [Yardım Merkezi](#) makalemizi inceleyin.

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. Ücret karşılığında cinsel eylemi tanıttığı veya teşvik ettiği anlaşılan uygulamalara veya uygulama içeriklerine izin verilmez. Cinsel açıdan yıkıcı ve taciz edici davranışlarla ilişkili içerikleri barındıran veya tanıtan ya da kişinin rızası dışında cinsel içerikleri dağıtan uygulamalara izin verilmez. Çıplaklık barındıran içeriklere, birincil amacı eğitim, belgesel, bilimsel veya sanatsal olup cinsel tatmine yönelik olmadıkları takdirde izin verilebilir.

Daha geniş bir içerik kataloğunun parçası olarak kitap/video listeleyen katalog uygulamaları, aşağıdaki şartlar karşılandığı takdirde cinsel içerik barındıran kitap (e-kitap ve sesli kitap dahil) veya video içeriklerini dağıtabilir:

- Cinsel içerik barındıran kitaplar/videolar, uygulamadaki genel kataloğun küçük bir kısmını oluşturmalıdır.
- Uygulama, cinsel içerik barındıran kitapları/filmleri aktif bir şekilde tanıtmamalıdır. Bu içerikler, kullanıcı geçmişine dayalı önerilerde veya genel fiyat promosyonlarında görünmeye devam edebilir.

- Uygulama; çocukları tehlikeye atan içerik, porno veya geçerli yasalar uyarınca yasa dışı olarak tanımlanmış başka cinsel içerikleri barındıran hiçbir kitabı/videoyu dağıtmamalıdır.
- Uygulama, cinsel içerik barındıran kitaplara/videolara erişimi kısıtlayarak küçükleri korumalıdır.

Bir uygulamada bu politikayı ihlal eden içerik olsa da bu içerik belirli bir bölgede uygun kabul ediliyor olabilir. Bu durumda uygulama o bölgedeki kullanıcılara sunulmaya devam ederken diğer bölgelerdeki kullanıcılar uygulamayı kullanamaz.

Yaygın görülen ihlallere ilişkin bazı örnekleri aşağıda bulabilirsiniz:

- Öznenin çıplak, bulanıklaştırılmış veya minimum düzeyde giyinik olduğu ve/veya giysinin 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
- Bir katılımcının başka bir katılımcıya para, hediye veya finansal destek sağlamasının veya talep etmesinin beklendiği veya ima edildiği ücret karşılığı buluşma veya cinsel içerikli görüşmeler (“sugar dating”) dahil ancak bunlarla sınırlı olmamak üzere cinsellikle ilgili eğlence, eskort hizmetleri veya ücret karşılığında cinsel eylemler sağlıyormuş gibi yorumlanabilecek diğer hizmetleri tanıtan uygulamalar
- Şaka ya da eğlence uygulaması olarak etiketlenmiş olsa bile kişileri çıplak gösterdiği veya elbiselerin içini gösterdiği iddiasında olan uygulamalar gibi kişileri aşağılayan veya nesneleştiren uygulamalar
- Habersiz çekilen fotoğraflar, gizli kamera, kişinin rızası dışında deepfake veya benzeri bir teknolojiyle oluşturulan cinsel içerikler ya da saldırı içerikleri gibi insanları cinsel açıdan tehdit etmeye veya istismar etmeye çalışan içerik veya davranışlar

Nefret Söylemi

Şiddeti özendiren veya ırk, etnik köken, din, engellilik, yaş, uyruk, gazilik durumu, cinsel yönelim, cinsiyet, cinsel kimlik veya sistematik ayrımcılık ya da ötekileştirmeyle 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 ilişkin bazı 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 veya 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 veya şiddet içeren tehditlerin grafik tasvirleri veya açıklamaları.
- Kendine zarar verme, intihar, yeme bozuklukları, boğulma oyunları veya ciddi yaralanma ya da ölümle sonuçlanabilecek diğer eylemleri teşvik eden uygulamalar.

Şiddet İçeren Aşırılık

Sivillere karşı şiddet eylemlerine karışan, hazırlanan veya bunların sorumluluğunu üstlenen terör örgütlerinin ya da diğer tehlikeli örgütlerin veya hareketlerin, üye alımı da dahil olmak üzere hiçbir amaçla Google Play'de uygulama yayınlamasına izin verilmez.

Şiddet barındıran aşırılıkla ilgili veya sivillere karşı şiddet eylemlerinin planlanması, hazırlanması veya yüceltilmesiyle alakalı içerik (terörist faaliyetleri destekleyen, şiddeti teşvik eden veya terör saldırılarını öven içerikler gibi) barındıran uygulamalara izin verilmez. Şiddet barındıran aşırılıkla ilgili içerikleri eğitsel, belgesel, bilimsel veya sanatsal amaçlarla yayınlıyorsanız alakalı eğitici, belgesel, bilimsel veya sanatsal bağlamı sağlamaya dikkat edin.

Hassas Olaylar

Sivil acil durumlar, doğal afetler, kamu sağlığını ilgilendiren acil durumlar, savaşlar, ölümler veya diğer trajik olaylar gibi önemli sosyal, kültürel ya da siyasi etkiye sahip hassas olaylara karşı hassasiyet göstermeyen veya bu tür olayları 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 ilişkin bazı örnekleri aşağıda bulabilirsiniz:

- Gerçek kişi veya kişilerin intihar, aşırı dozda uyuşturucu kullanımı, doğal nedenler gibi sebeplere bağlı olarak ölmelerine hassasiyet göstermeme
- Belgelerle gerçekliği kanıtlanmış 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 ilişkin bazı 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 vermez.

- 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 vermeyiz.

Yaygın görülen ihlallere ilişkin bazı örnekleri aşağıda bulabilirsiniz:

- Uygulama içi alışveriş sepeti özelliği ile kullanıcıların marihuana siparişi vermelerine izin verme.
- 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

Nikotin içeren ürün (ör. e-sigara ve nikotin poşetleri) veya tütün satışını kolaylaştıran ya da alkol, tütün veya nikotin yasa dışı veya uygunsuz kullanımını teşvik eden uygulamalara izin verilmez.

Ek bilgiler

- Küçüklere alkol veya tütün kullanımı ya da satışının anlatılmasına veya teşvik edilmesine izin verilmez.
- Tütün tüketiminin sosyal, cinsel, mesleki, entelektüel veya sportif gücü artırabileceğinin ima edilmesine izin verilmez.
- Aşırı veya uzun süreli içki tüketimi ya da içki yarışmalarının olumlu gösterilmesi de dahil olmak üzere aşırı içki tüketiminin tanıtımının yapılmasına izin verilmez.
- Tütün ürünlerinin reklamına, tanıtımına veya belirgin bir şekilde öne çıkarılmasına (tütün satan sitelere yönlendiren bağlantılar, reklamlar, banner'lar ve kategoriler dahil) izin verilmez.
- Tütün ürünlerinin bazı bölgelerde gıda/market alışveriş uygulamalarında sınırlı satışına izin verilebilir. Bu satışlar, yaş denetimine ve teslimat sırasında kimlik kontrolü gibi önlemlere tabidir.
- Yaş denetimiyle ilgili güvenlik önlemlerine tabi olup nikotin bırakma yardımcıları olarak pazarlanan ürünlerin satışına izin verilebilir.

Mali Hizmetler

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

Bu politikanın amacı doğrultusunda, para ve kripto para birimlerinin yönetimi veya yatırımıyla ilgili ürün ve hizmetler (kişiyi 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 içermek) uymanız gereklidir.

Finansal özellikler içeren tüm uygulamalar [Play Console](#)'daki Finansal Özellikler Beyan Formu'nu doldurmalıdır.

İkili Opsiyonlar

Kullanıcılara ikili seçenek ticareti yapma olanağı sağlayan uygulamalara izin verilmez.

Bireysel krediler

Bireysel krediler bir şahıs, 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, taraflar arası krediler, ipotekli krediler
- Dahil olmayan örnekler: konut finansmanı kredileri, taşıt 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, Play Console'daki uygulama kategorisini "Finans" olarak ayarlamalı ve uygulama meta verilerinde aşağıdaki bilgileri paylaşmalıdır:

- Minimum ve maksimum geri ödeme süresi
- Genellikle bir yıllık faiz oranı, ücretler ve diğer masrafların toplanmasından oluşan maksimum yıllık faiz oranı veya yerel yasalar çerçevesinde hesaplanmış benzer başka bir oran
- Ana para ve 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 (Bu politikada belirtilen kısıtlamalara tabidir.)

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.

Belirli yönetmeliklerin, mevcut yasal çerçeveler kapsamında bu tür kısa vadeli kredi verme uygulamalarına açıkça izin verdiği ülkelerde faaliyet gösteren bireysel kredi uygulamaları için bu politikayla ilgili istisnalar göz önünde bulundurulacaktır. İstisnalar, bu nadir durumlarda ilgili ülkenin geçerli yerel yasalarına ve yönetmeliklerine uygun olarak değerlendirilecektir.

Bireysel kredi hizmeti verme yetkinizi kanıtlamak için sunduğunuz lisans veya belgeler ile geliştirici hesabınız arasında bağlantı kurabilmemiz gerekir. Hesabınızın tüm yerel yasalarla ve yönetmeliklerle uyumlu olduğunu onaylamak için ek bilgi veya belgeler istenebilir.

Bireysel kredi uygulamaları, birincil işlevi bireysel kredilere erişimi kolaylaştırmak olan uygulamalar (örneğin, olası satış yaratanlar veya kolaylaştıranlar), kredi aracı uygulamaları (kredi hesaplayıcıları, kredi kılavuzları vb.) ve ücret erişimi (EWA) uygulamalarının fotoğraflar ve kişiler gibi hassas verilere erişmesi yasaktır. Aşağıdaki izinler yasaklanmıştır:

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

Hassas bilgileri veya API'leri kullanan uygulamalar ek kısıtlamalara ve şartlara tabidir. Daha fazla bilgi için lütfen [İzinler Politikası](#)'na bakın.

Yıllık faiz oranı yüksek bireysel krediler

ABD'de yıllık faiz oranı %36 veya daha yüksek bireysel kredi uygulamalarına izin vermeyiz. ABD'deki bireysel kredi uygulamaları, [Kredilerde Doğru Bilgilendirme Yasası \(TILA\)](#) uyarınca hesaplanmış maksimum yıllık faiz oranlarını göstermelidir.

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

Ülkelere özgü koşullar

Belirtilen ülkeleri hedefleyen bireysel kredi uygulamaları ek şartlara uymalı ve [Play Console](#)'daki Finansal Özellikler Beyan Formu kapsamında ek dokümanlar sunulmalıdır. Google Play'in talep etmesi halinde, ilgili yönetmelik ve lisanslama şartlarına uygunluğunuza dair ek bilgi veya dokümanları sağlamanız gerekir.

1. Hindistan

- Bireysel kredi sağlamak için Hindistan Merkez Bankası (RBI) lisansına sahipseniz inceleyebilmemiz amacıyla lisansınızın bir kopyasını göndermeniz gerekir.
- Doğrudan borç verme faaliyetlerinde yer almayıp yalnızca kayıtlı Banka Dışı Finansal Şirketler (NBFC'ler) veya bankalar tarafından kullanıcılara borç verilmesini kolaylaştıracak bir platform sağlıyorsanız bu durumu beyanda doğru bir şekilde yansıtmamız gerekir.
 - Ayrıca, kayıtlı tüm NBFC'lerin ve bankaların adları, uygulamanızın açıklamasında belirgin bir şekilde paylaşılmalıdır.

2. Endonezya

- Uygulamanız, 77/POJK.01/2016 No.lu OJK Yönetmeliği (zaman zaman değiştirilebilir) çerçevesinde Bilgi Teknolojilerine Dayalı Kredi Hizmetleri sunuyorsa incelememiz için geçerli lisansınızın bir kopyasını göndermeniz gerekir.

3. Filipinler

- Online Kredi Platformları (OLP) aracılığıyla kredi veren tüm finans ve kredi şirketleri, Filipinler Menkul Kıymetler ve Borsa Komisyonu'ndan (PSEC) SEC Kayıt Numarası ve Yetki Belgesi (CA) almalıdır.
 - Ayrıca, uygulamanızın açıklamasında Şirket Adınızı, İşletme Adınızı, PSEC Kayıt Numaranızı ve Finans/Kredi Şirketi Çalıştırmak İçin Yetki Belgenizi (CA) paylaşmanız gerekir.
- Taraflar arası (P2P) kredi gibi veya Kitle Fonlaması İçin Geçerli Kurallar ve Yönetmelikler'de (CF Kuralları) tanımlandığı şekilde krediye dayalı kitle fonlaması faaliyetlerinde bulunan uygulamalar, işlemleri PSEC Kayıtlı CF Aracıları üzerinden gerçekleştirmelidir.

4. Nijerya

- Dijital borç verenler (DML), Nijerya Federal Rekabet ve Tüketici Koruma Komisyonu'nun (FCCPC) zaman zaman değiştirilebilen 2022 tarihli DİJİTAL BORÇ VERME İÇİN SINIRLI GEÇİCİ YÖNETMELİK/TESCİL ÇERÇEVESİ VE YÖNERGELERİ'ne uymalı, bunları yerine getirmeli ve FCCPC'den doğrulanabilir bir onay mektubu almalıdır.
- Kredi Toplayıcılar, dijital borç hizmetlerine dair doküman ve/veya sertifika ile birlikte iş ortaklığı olan her DML için iletişim bilgisi sağlamalıdır.

5. Kenya

- Dijital kredi verenler (DCP), DCP tescil işlemini tamamlamalı ve Kenya Merkez Bankası'ndan (CBK) lisans almalıdır. CBK'dan alınan lisansın bir kopyası, beyana eklenmelidir.
- Doğrudan borç verme faaliyetlerinde yer almayıp yalnızca kayıtlı DCP'ler tarafından kullanıcılara borç verilmesini kolaylaştıracak bir platform sağlıyorsanız bu durumu beyanda doğru bir şekilde yansıtmamız ve ilgili iş ortaklarınızın DCP lisansının kopyasını eklemeniz gerekir.
- Şu an için yalnızca CBK'nın resmi web sitesindeki Dijital Kredi Verenler Dizini'nde yer alan tüzel kişilerin beyanları ve lisansları kabul edilmektedir.

6. Pakistan

- Kredi veren her banka dışı finansal şirket (NBFC) yalnızca bir dijital kredi verme uygulaması (DLA) yayınlabilir. NBFC başına birden fazla DLA yayınlamaya çalışan geliştiriciler, geliştirici hesaplarının ve ilişkili diğer hesapların feshedilmesi riskini almış olurlar.

- Pakistan'da dijital kredi verme hizmeti sunmak veya kolaylaştırmak için SECP'den alınmış onay belgesi sunmanız gerekir.

7. Tayland

- Tayland'ı hedefleyen ve faiz oranı en az %15 olan bireysel kredi uygulamaları, Bank of Thailand'den (BoT) veya Maliye Bakanlığı'ndan (MoF) geçerli bir lisans almalıdır. Geliştiriciler Tayland'da bireysel kredi sağlayabileceklerini veya bireysel kredi almayı kolaylaştırabileceklerini kanıtlayan dokümanlar sunmalıdır. Bu kapsamda:
 - Bireysel kredi sağlayıcı ya da nano finans kuruluşu olarak faaliyet gösterebileceklerini kanıtlamak için Bank of Thailand'den alınmış lisansın bir kopyası sunulmalıdır.
 - Pico veya Pico-plus düzeyinde kredi veren kuruluş olarak faaliyet göstermek için Maliye Bakanlığı'ndan alınmış Pico-finance işletme ruhsatının bir kopyası sunulmalıdır.

Aşağıda, yaygın görülen bir ihlale ilişkin örneği bulabilirsiniz:

[< Back](#)



Easy Loans
offers in app purchases

 1255

Install

Are you looking for a speedy loan?

Easy Loans Finance can help you get cash in your bank account in an hour!

- Get cash sent to your bank account!
- Safe and easy
- Great short-term rate
- Fast lender approval
- Easy to use
- Loan delivered in an hour
- Download our app and get cash easy!

Violations

No minimum and maximum period for repayment

Doesn't disclose Maximum Annual Percentage Rate (APR), which generally includes interest rate plus fees and other costs for a year, or similar other rate calculated consistently with local law

No representative example of the total cost of the loan, including all applicable fees

Gerçek Parayla Kumar Oynama, Oyunlar ve Yarışmalar

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

Kumar Uygulamaları

Kısıtlamalara ve tüm Google Play politikalarına uymaya tabi olmak şartıyla, belirli 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 online kumar ürünleri içeren, geçerli lisansa sahip veya yetkili kumar uygulamalarına izin verilir.

- Çevrimiçi Kumarhane oyunları
- Spor Bahisleri
- At Yarışı (Spor Bahisleri'nden ayrı bir şekilde düzenlendiği ve lisanslandığı durumlarda)
- Piyangolar
- Günlük Fantezi Spor

Uygun uygulamalar aşağıdaki gereksinimleri karşılamalıdır:

- Geliştirici, uygulamayı Play'de dağıtabilmek 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 İçerik Faturalandırma hizmetini kullanmamalıdır;
- Uygulama, Google Play Store'dan ücretsiz olarak indirilip yüklenebilmelidir;
- Uygulamanın AO (Yalnızca Yetişkinler İçin) veya [IARC eş değeri](#) bir derecelendirmeye sahip olması gerekir ve
- Uygulamada ve uygulamanın girişinde, sorumluluğunu bilerek kumar oynamaya ilgili bilgiler açıkça gösterilmelidir.

Diğer Gerçek Parayla Oynanan Oyunlar, Yarışmalar ve Turnuva uygulamaları

Kumar uygulamalarıyla ilgili yukarıda belirtilen uygunluk koşullarını karşılamayan ve aşağıdaki "Gerçek Parayla Oynanan Diğer Oyun Pilotları" listesine dahil edilmeyen 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 kapsam yalnızca bunlarla sınırlı değildir (aşağıda açıklanan Oyunlaştırılmış Bağlılık Programları şartları 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 kullanıcılara 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.

Gerçek Parayla Oynanan Diğer Oyun Pilotları

Belirli bölgelerde, gerçek parayla oynanan bazı oyun türleri için sınırlı süreli pilot programlar yürütebiliriz. Ayrıntılar için şu [Yardım Merkezi sayfasına](#) göz atın. Japonya'daki online oyuncak kapma oyunu pilot programı 11 Temmuz 2023'te sona erdi. Online oyuncak kapma oyunu uygulamaları 12 Temmuz 2023'ten itibaren, geçerli yasaya ve belirli [şartlara](#) tabi olarak dünya genelinde Google Play'de gösterilebilir.

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 ödüller; 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:

- Uygun bir parasal işlemle ilişkilendirilen avantajlar, ayrıcalıklar veya ödüller sunan bağlılık puanları ya da 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 koşullarında 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 koşullarında 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 koşullarında açıkça belirtin.

Bağlılık programı sunan uygulama türü	Bağlılık programının oyunlaştırılması ve değişken ödüller	Sabit bir orana/programa dayalı bağlılık ödülleri	Bağlılık programının Şartlar ve Koşullar gereksinimi	Şartlar ve Koşullar'da, şansa dayalı bağlılık programının kazanma olasılıkları veya seçim yöntemi açıklanmalıdır
Oyun	İzin Verilmez	İzin Verilir	Zorunlu	Yok (Oyun uygulamalarının bağlılık 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:

- Uygulama ve reklam (reklamverenler dahil), reklamın gösterildiği konum için geçerli tüm yasalara ve endüstri standartlarına uymalıdır;
- Reklam, tanıtılmakta olan kumarla ilgili tüm ürünlere ve hizmetlere ilişkin geçerli tüm yerel reklam lisans gereksinimlerini karşılamalıdır;
- Uygulama, 18 yaşından küçük olduğu bilinen kişilere kumarla ilgili reklam göstermemelidir;
- Uygulama, Aileler için programına kayıtlı olmamalıdır;
- Uygulama 18 yaşından küçük bireyleri hedeflememelidir;
- 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;
- Uygulamada kumar simülasyonu içeriği (ör. sosyal kumarhane uygulamaları, sanal slot makinesi içeren uygulamalar) sağlanmamalıdır;
- 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) sağlanmamalıdır;
- Uygulama içeriği, kumar ya da gerçek parayla oynanan oyun, piyango veya turnuva hizmetlerinin tanıtımını yapmamalı veya kullanıcıları bu hizmetlere yönlendirmemelidir

Yalnızca belirtilen bölümdeki (yukarıda) tüm gereksinimleri karşılayan uygulamalar kumar veya gerçek parayla oynanan oyun, piyango ya da turnuva reklamları içerebilir. Kabul edilen Kumar Uygulamaları (yukarıda tanımlandığı gibi) veya yukarıdaki 1-6 arası gereksinimleri karşılayan, kabul edilen Günlük Fantezi Spor 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
- [Yanıltıcı 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) ABD dışındaki ülkelerde yukarıda belirtilen Kumar Uygulamaları gereksinimleri ve başvuru sürecine uygun olmalıdır;
- 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](#);

- Uygulamada ve uygulamanın girişinde sorumluluğunu bilerek kumar oynamayla ilgili bilgiler açıkça gösterilmelidir;
 - 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 vermeyiz.

Yaygın görülen ihlallere ilişkin bazı örnekleri aşağıda bulabilirsiniz:

- Yasa dışı uyuşturucuları 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.

Kullanıcıları bir UGC platformuna yönlendirmeye yarayan özel tarayıcılar veya istemciler olan uygulamalar da dahil olmak üzere UGC barındıran veya öne çıkaran uygulamalar aşağıdaki şartları karşılayan sağlam, etkili ve kesintisiz UGC moderasyonu uygulamalıdır:

- Kullanıcıların UGC'yi oluşturabilmesi veya yükleyebilmesi için önce uygulamanın kullanım şartlarını ve/veya kullanıcı politikasını kabul etmesini gerektirmelidir;
- Sakıncalı içeriği ve davranışları tanımlamalı (Google Play Geliştirici Program Politikaları'na uygun şekilde) ve uygulamanın kullanım şartlarında veya kullanıcı politikalarında bunları yasaklamalıdır;
- Uygulamanın barındırdığı UGC, UGC türüyle tutarlı ve makul bir kontrol mekanizmasına tabi olmalıdır. Buna, sakıncalı UGC'leri ve kullanıcıları bildirip engellemek için uygulama içi bir sistem sağlamak ve gerektiğinde o UGC veya kullanıcı hakkında işlem yapmak da dahildir. Farklı UGC'ler için farklı kontrol mekanizmaları gerekebilir. Örneğin:
 - Kullanıcı doğrulama veya çevrimdışı kayıt gibi yöntemlerle belirli bir kullanıcı grubunun kimliğini tanımlayan UGC'lerin bulunduğu uygulamalar (ör. yalnızca belirli bir okul veya şirkette kullanılan uygulamalar), uygulama içinde içerikleri ve kullanıcıları bildirme işlevi sunmalıdır.
 - Belirli kullanıcılarla 1:1 etkileşime olanak tanıyan UGC özellikleri (ör. doğrudan mesajlaşma, etiketleme, bahsetme vb.), uygulama içinde kullanıcıları engelleme işlevi sunmalıdır.
 - Herkesin erişimine açık UGC'lere erişim sağlayan uygulamalar (ör. sosyal ağ uygulamaları ve blog yazarı uygulamaları), uygulama içinde kullanıcıları ve içerikleri bildirme ve kullanıcıları engelleme işlevi sunmalıdır.
 - Artırılmış gerçeklik (AR) uygulamaları söz konusu olduğunda, UGC moderasyonu (uygulama içi raporlama sistemi dahil) hem sakıncalı AR UGC'den (örneğin müstehcen bir AR görüntüsü) hem de hassas AR sabitleme konumundan sorumlu olmalıdır (örneğin askeri üs gibi erişimi sınırlı bir alana veya AR sabitlemenin mülk sahibi için sorun yaratabileceği özel mülke sabitlenmiş AR içeriği);
- Uygulama içi para kazanmanın sakıncalı kullanıcı davranışını teşvik etmesini engelleyen önlemler sağlamalıdır.

Arızı Cinsel İçerik

(1) Ağırlıklı olarak cinsel olmayan içeriklere erişim sunan ve (2) cinsel içerikleri aktif bir şekilde tanıtmayan veya önermeyen UGC uygulamalarında yer alan cinsel içerikler "arızı" olarak kabul edilir. Geçerli kanunlarca yasa dışı olarak tanımlanan cinsel içerikler ve [çocukların tehlikeye atıldığı](#) içerikler "arızı" olarak kabul edilmez ve bu içeriklere izin verilmez.

Aşağıdaki şartların tamamı karşılandığı sürece UGC uygulamalarında arızı cinsel içerikler yer alabilir:

- Bu tür içerikler, tamamen devre dışı bırakılması için kullanıcının en az iki işlem yapmasını gerektiren filtrelerin arkasında varsayılan olarak gizlenmelidir (Örneğin, kod karartan bir geçiş reklamının arkasında saklanmalı veya "güvenli arama" devre dışı bırakılmadıysa varsayılan olarak görüntülenmesi engellenmelidir).
- [Aile Politikası](#)'nda tanımlandığı üzere çocukların, [yönlendirmesiz yaş seçim ekranı](#) veya geçerli kanunlarca tanımlanmış uygun bir sistem gibi yaş filtreleme sistemleri kullanılarak uygulamanıza erişimleri açıkça engellenmelidir.
- Uygulamanız, [İçerik Derecelendirmesi Politikası](#) uyarınca, içerik derecelendirmesi anketinin UGC ile ilgili sorularına doğru yanıtlar vermelidir.

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.

Sağlık İçerikleri ve Hizmetleri

Kullanıcıları zararlı sağlık içeriklerine ve hizmetlerine maruz bırakan uygulamalara izin verilmez.

Uygulamanız sağlık içerikleri ve hizmetleri sunuyorsa veya bunların tanıtımını yapıyorsa geçerli yasalara ve yönetmeliklere uygun olmasını sağlamanız gerekir.

Sağlık Uygulamaları

Sağlık verilerine erişen ve [sağlık uygulaması](#) olan ya da sağlıkla alakalı özellikler sunan uygulamalar, aşağıdaki şartlara ek olarak [Gizlilik, Yanıltma ve Cihazların Kötüye Kullanımı](#) ile Hassas Olaylar da dahil olmak üzere mevcut Google Play Geliştirici Politikaları'na uymak zorundadır:

- Console Beyanı:**
 - Play Console'daki Uygulama içeriği sayfasına (Politika > Uygulama içeriği) giderek uygulamanızın ait olduğu kategoriyi veya kategorileri seçin.
- Gizlilik Politikası ve Belirgin Açıklama Şartları:**
 - Uygulamanız Play Console'da belirtilen alanda bir gizlilik politikası bağlantısı, uygulamanın kendi içinde de bir gizlilik politikası bağlantısı veya metni yayınlamalıdır. Lütfen gizlilik politikanızın çalışan, herkesin erişimine açık ve coğrafi sınıra tabi olmayan bir URL'de bulunduğundan (PDF kabul edilmez.) ve düzenlenebilir olmadığından emin olun ([Veri Güvenliği bölümü](#) uyarınca).
 - Uygulama içi açıklamalarla birlikte uygulamanızın gizlilik politikasında; uygulamanızın, yukarıdaki Veri Güvenliği bölümünde açıklanan verilerle sınırlı olmamak üzere [kişisel veya hassas kullanıcı](#)

[verilerine](#) nasıl eriştiği, bu verileri nasıl topladığı, kullandığı ve paylaştığı kapsamlı bir şekilde açıklanmalıdır. Uygulama, [tehlikeli veya çalışma zamanında istenen izinler](#) tarafından denetlenen işlevler ve veriler için geçerli tüm [belirgin açıklama ve rıza şartlarını](#) karşılamalıdır.

- Sağlık uygulamasının temel işlevini yerine getirmesi için gerekli olmayan izinlerin istenmemesi ve kullanılmayan izinlerin kaldırılması gerekir. Sağlıkla alakalı hassas veri kapsamına giren izinlerin listesini [Sağlık uygulaması kategorileri ve ek bilgiler](#) başlıklı makalede bulabilirsiniz.
- Uygulamanız aslında sağlık uygulaması değilse ancak sağlıkla alakalı özellikler içeriyor ve sağlık verilerine erişiyorsa yine de Sağlık Uygulaması Politikası kapsamına girer. Uygulamanın temel işlevi ile sağlıkla alakalı verilerin toplanması arasındaki bağlantı, kullanıcı için net olmalıdır (ör. sigorta sağlayıcılar, oyunda ilerlemeye izin vermek için kullanıcının etkinlik verilerini toplayan oyun uygulamaları vb.). Uygulamanın gizlilik politikası, bu sınırlı kullanımı yansıtmalıdır.

• Ek şartlar:

Sağlık uygulamanız aşağıdaki kategorilerden birine giriyorsa ilgili şartlara uymanız ve Play Console'da doğru kategoriye seçmeniz gerekir:

- **Devlet kuruluşlarıyla ilişkili sağlık uygulamaları:** Bir devlet kuruluşundan veya onaylı bir sağlık kuruluşundan kendileriyle ilişkili bir uygulama geliştirme ve dağıtma konusunda izniniz varsa [Ön Bildirim Formu](#)'nu kullanarak uygunluk belgenizi göndermeniz gerekir.
- **Temas izleme/sağlık durumu uygulamaları:** Uygulamanız temas izleme ve/veya sağlık durumu uygulaması ise lütfen Play Console'da "Hastalık Önleme ve Halk Sağlığı"nı seçip yukarıdaki ön bildirim formunu kullanarak gerekli bilgileri sağlayın.
- **İnsan deneyleri araştırma uygulamaları:** İnsanlar üzerinde tıbbi araştırmalar yapan uygulamalar, katılımcılara gereken bilgileri sunarak onaylarını almak, katılımcı küçükse ebeveynlerin veya velilerinin iznini almak da dahil olmak üzere tüm kurallara ve tüzüklere uymalıdır. Sağlık araştırması uygulamaları ayrıca herhangi bir nedenle muaf olmadıkları takdirde Kurumsal İnceleme Kurulu (IRB) ve/veya dengi bir bağımsız etik komitesinden onay almış olmalıdır. Talep edilmesi halinde bu onayın belgelenmesi zorunludur.
- **Tıbbi cihaz veya tıbbi cihaz olarak yazılım (SaMD) uygulamaları:** Tıbbi cihaz ya da tıbbi cihaz olarak yazılım kapsamına giren uygulamalar, sağlık uygulamasının yönetimi ve uygunluğundan sorumlu bir düzenleyici makam ya da kurumdan izin belgesi ya da başka bir onay belgesi alıp saklamalıdır. Bu tür izin veya onay belgeleri istendiğinde sunulmalıdır.

Health Connect Verileri

Health Connect izinleri üzerinden erişilen veriler, kişisel ve hassas kullanıcı verisi olarak değerlendirilmekle birlikte [Kullanıcı Verileri](#) Politikası'na ve [ek şartlara](#) tabidir.

Reçeteli İlaçlar

Reçeteli ilaçların reçetesiz satışını veya satın alınmasını kolaylaştıran uygulamalara izin verilmez.

Onaylanmamış Maddeler

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

Yaygın görülen ihlallere ilişkin bazı örnekleri aşağıda bulabilirsiniz:

- [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.

Sağlıkla İlgili Yanlış Bilgilendirme

Mevcut tıbbi mutabakatla çelişen veya başkalarına zarar verebilecek şekilde sağlıkla ilgili yanıltıcı iddialar içeren uygulamalara izin verilmez.

Yaygın görülen ihlallere ilişkin bazı örnekleri aşağıda bulabilirsiniz:

- Aşılarla ilgili yanıltıcı iddialar (ör. aşılardan kişinin DNA'sını değiştirebileceği iddiası)
- Onaylanmamış zararlı tedavilerin savunulması
- Sağlıkla ilgili diğer zararlı uygulamaların (ör. dönüşüm terapisi) savunulması

Tıbbi İşlevler

Tıp veya sağlıkla ilgili işlevleri olan ancak yanıltıcı ya da zararlı olabilecek uygulamalara izin verilmez. Örneğin, yalnızca uygulamaya dayalı olarak oksimetre işlevi sunduğunu iddia eden uygulamalara izin verilmez. Oksimetre uygulamaları; oksimetre işlevini desteklemek üzere tasarlanmış harici donanımlar, giyilebilir cihazlar veya akıllı telefonlarda yerleşik olarak bulunan özel sensörlerle desteklenmelidir. Ayrıca bu desteklenen uygulamaların meta verilerinde, uygulamanın tıbbi kullanım için olmadığını, yalnızca genel fitness ile sağlık için tasarlandığını ve tıbbi cihaz olmadığını belirten sorumluluk reddi beyanları yer almalıdır. Uyumlu donanım modeli/cihaz modeli de düzgün bir şekilde açıklanmalıdır.

Ödemeler - Klinik Hizmetleri

Düzenlemeye tabi klinik hizmetleriyle ilgili işlemlerde Google Play'in faturalandırma sistemi kullanılmamalıdır. Daha fazla bilgi için [Google Play'in Ödeme Politikası'nı anlama](#) bölümüne bakın.

Blok zincirine dayanan içerik

Blok zinciri teknolojisi hızla gelişmeye devam ediyor. Amacımız, geliştiricilerin kullanıcılara daha zengin ve ilgi çekici deneyimler sunarak yeniliklerle başarıya ulaşacakları bir platform sağlamaktır.

Bu politikanın amacı doğrultusunda, blok zinciri tabanlı içerikler, blok zincirinde tutulan token atanmış dijital varlıklar olarak değerlendirilir. Uygulamanızda blok zinciri tabanlı içerikler varsa bu şartlara uymanız gerekir.

Kripto para borsaları ve yazılım cüzdanları

Kripto para birimlerini satın alma, bulundurma veya bozdurma işlemleri, yasal düzenlemelere tabi yargı alanlarında yetkili hizmetler aracılığıyla yapılmalıdır.

Ayrıca, uygulamanızın hedeflediği tüm bölge veya ülkelerde geçerli tüzüklere uymalı, ürün ve hizmetlerinizin yasaklandığı yerlerde uygulamanızı yayınlamamalısınız. Google Play, geçerli tüzüklerle veya lisanslamayla ilgili şartlara uyduğunuzu gösteren ek bilgiler veya dokümanlar sunmanızı isteyebilir.

Kripto para madenciliği

Cihazlarda kripto para birimi madenciliğine izin vermeyiz. Kripto para birimi madenciliğini uzaktan yöneten uygulamalara izin veririz.

Token Atanmış Dijital Varlıklarla İlgili Şeffaflık Şartları

Uygulamanız, token atanmış dijital varlıkları kullanıcılara satıyor veya bunları kazanmalarını sağlıyorsa Play Console'un Uygulama İçeriği sayfasındaki Finansal Özellikler Beyan Formu'nu doldurarak bunu beyan etmeniz gerekir.

Uygulama içi ürün oluştururken ürün ayrıntılarında bunun token atanmış bir dijital varlığı temsil ettiğini belirtmeniz gerekir. Daha fazla bilgi için [Uygulama içi ürün oluşturma](#) başlıklı makaleyi inceleyebilirsiniz.

Oynama veya alım satım faaliyetlerinden elde edilebilecek herhangi bir potansiyel kazancı tanıtamaz veya övemezsiniz.

NFT oyunlaştırma için ek şartlar

Google Play'in [Gerçek Parayla Kumar Oynama, Oyunlar ve Yarışmalar Politikası](#) uyarınca, NFT'ler gibi token atanmış dijital varlıkları entegre eden kumar uygulamaları, başvuru sürecini tamamlamalıdır.

Kumar uygulamalarıyla ilgili uygunluk koşullarını karşılamayan ve [Gerçek Parayla Oynanan Diğer Oyun Pilotları](#) listesine dahil edilmeyen diğer uygulamaların hiçbirinde kullanıcıların maddi değere sahip herhangi bir şey karşılığında değeri bilinmeyen bir NFT almasına izin verilmemelidir. Kullanıcılar tarafından satın alınan NFT'ler, oyun içinde kullanıcıların deneyimini iyileştirmek veya ilerlemelerine yardımcı olmak için kullanılmalıdır. NFT'ler, gerçek dünyada maddi değeri olan ödüller (başka NFT'ler dahil) kazanmak için bahis yapmak amacıyla kullanılamaz.

Yaygın görülen ihlallere ilişkin bazı örnekleri aşağıda bulabilirsiniz:

- NFT paketi satan ancak paketin tam içeriğini ve NFT'lerin değerini açıklamayan uygulamalar
- Parayla oynanan ve ödül olarak NFT veren sosyal kumar oyunları (ör. slot makineleri)

Yapay zeka tarafından üretilmiş içerik

Üretken yapay zeka modelleri, geliştiriciler tarafından gittikçe daha fazla kullanılıyor. Siz de etkileşimi artırmak ve kullanıcı deneyimini iyileştirmek için uygulamalarınızda bu modelleri kullanıyor olabilirsiniz. Google Play'in amacı, yapay zeka tarafından üretilmiş içeriğin tüm kullanıcılar için güvenli olmasını ve kullanıcı geri bildirimleri dikkate alınarak sorumluluk bilinciyle yenilik yapılmasını sağlamaktır.

Yapay zeka tarafından üretilmiş içerik

Yapay zeka tarafından üretilmiş içerik, üretken yapay zeka modellerinin kullanıcı istemlerine dayalı olarak oluşturduğu içeriktir. Yapay zeka tarafından üretilmiş içeriklere örnekler:

- Yazılı etkileşime dayalı, üretken yapay zeka destekli chatbot'lar (Chatbot ile etkileşim, uygulamanın ana özelliğidir.)
- Yazılı, resimli veya sesli istemlere dayalı olarak yapay zeka tarafından üretilen resimler

Kullanıcı güvenliğini sağlamak için ve Google Play'in [Politika Kapsamı](#) uyarınca, yapay zeka kullanarak içerik üreten uygulamalar mevcut Google Play Geliştirici Politikaları'na uymalıdır. [Çocukların istismar veya taciz edilmesini kolaylaştıran içerikler](#) gibi [kısıtlı içeriklerin](#) ve [yanıltıcı davranışlara](#) olanak tanıyan içeriklerin üretilmesini yasaklamak ve engellemek de buna dahildir.

Yapay zeka kullanarak içerik üreten uygulamalarda, kullanıcıların uygulamadan çıkmasına gerek kalmadan rahatsız edici içerikleri geliştiricilere bildirebilmesi veya işaretleyebilmesi için kullanıcı bildirme ya da işaretleme özellikleri bulunmalıdır. Geliştiriciler, kullanıcı bildirimlerinden yararlanarak uygulamalarında içerik filtreleme ve kontrol mekanizmalarını düzenlemelidir.

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 bildirim](#) gönderin.

Bir ticari marka sahibiyseniz 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 ihlalden dolayı 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.

Yaygın görülen ihlallere ilişkin bazı örnekleri aşağıda bulabilirsiniz:

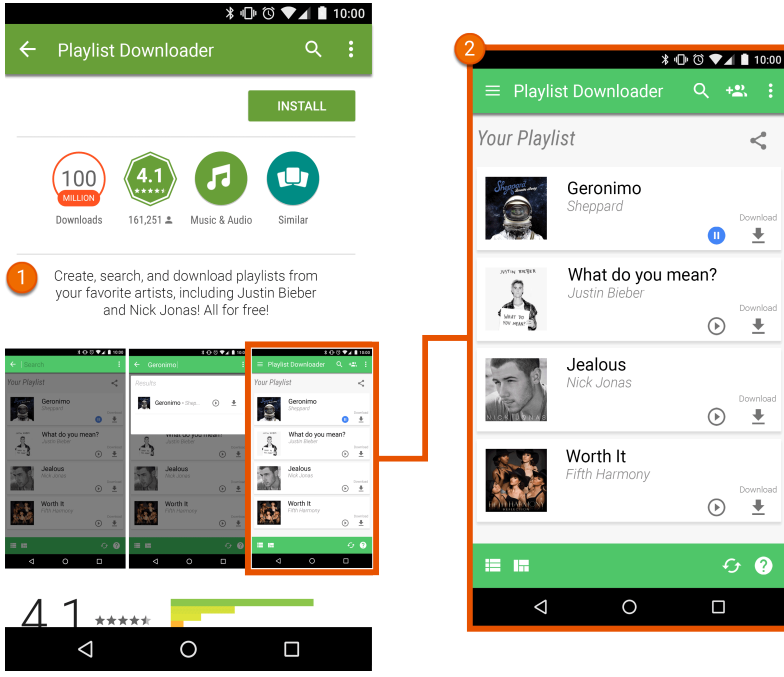
- Müzik albümleri, video oyunlar ve kitapların kapak resimleri.
- Filmler, televizyon şovları veya video oyunların pazarlama resimleri.
- Çizgi romanlar, çizgi filmler, filmler, müzik videoları veya televizyon şovlarından çizimler veya resimler.
- Okul ve profesyonel spor takımlarının logoları.
- Kamuya 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 olmayacağını 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 vermeyiz. 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. cihaz bilgileri de dahil bir kullanıcıdan alınan veya kullanıcı hakkında toplanan bilgiler) nasıl kullandığınız konusunda şeffaf olmalısınız. Bu gereklilik, uygulamanızdan kullanıcı verilerine erişim, verileri toplama, kullanma, işleme ve paylaşma süreçlerinin açıklanması ve verilerin yalnızca politikaya uygun olduğu belirtilen amaçlarla kullanılması anlamına gelir. Kişisel ve hassas kullanıcı verilerinin işlenmesinin aşağıdaki "Kişisel ve Hassas Kullanıcı Verileri" bölümünde yer alan ek

şartlara da tabi olduğunu unutmayın. Bu Google Play şartları, geçerli gizlilik ve veri koruma yasalarında belirtilen şartlara ek olarak uygulanır.

Uygulamanıza üçüncü taraf kodu (ör. bir SDK) eklerseniz uygulamanızda kullanılan üçüncü taraf kodunun ve bu üçüncü tarafın uygulamanızdaki kullanıcı verileriyle ilgili yaklaşımının, kullanım ve açıklama şartları da dahil olmak üzere Google Play Geliştirici Program Politikaları'na uygun olmasını sağlamanız gerekir. Örneğin, SDK sağlayıcılarınızın uygulamanızdaki kişisel ve hassas kullanıcı verilerini satmamasını sağlamalısınız. Bu şart hem sunucuya gönderildikten sonra aktarılan hem de uygulamanıza üçüncü taraf kodu yerleştirilerek aktarılan kullanıcı verileri için geçerlidir.

Kişisel ve Hassas Kullanıcı Verileri

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, [sağlık verileri](#) , [Health Connect](#) verileri, cihazdaki diğer uygulamaların envanteri, mikrofon, kamera ve diğer hassas cihaz veya kullanım verilerini içerir ancak bunlarla sınırlı değildir. Uygulamanız kişisel ve hassas kullanıcı verilerini işliyorsa şunları yapmalısınız:

- Uygulama aracılığıyla edinilen kişisel ve hassas kullanıcı verileriyle ilgili erişim, toplama, kullanım ve paylaşım sürecini, uygulama ve hizmet işleviyle ve makul ölçüde kullanıcıdan beklenebilecek politikaya uygun amaçlarla sınırlandırmalısınız:
 - Kişisel ve hassas kullanıcı verilerinin kullanım kapsamını reklam yayınlamak için genişleten uygulamalar, Google Play'in [Reklam Politikası](#) 'na uygun olmalıdır.
 - Ayrıca, gereken durumlarda [servis sağlayıcılara](#) da veri aktarabilirsiniz. Buna ek olarak, geçerli bir resmi makam talebine veya yasaya uymak gibi yasal nedenlerle ya da birleşme veya satın alma kapsamında (kullanıcılara yasal olarak uygun şekilde bilgilendirme yaparak) veri aktarabilirsiniz.
- Modern kriptografi kullanarak iletme (örneğin, HTTPS üzerinden) de dahil olmak üzere tüm kişisel ve hassas kullanıcı verilerini güvenli bir şekilde işlemelisiniz.
- Mümkün olduğunda her zaman, [Android izinleriyle](#) korunan verilere erişmeden önce çalışma zamanı izni istemelisiniz.
- Kişisel ve hassas kullanıcı verilerini satmamalısınız.
 - "Satış", kişisel ve hassas kullanıcı verilerinin para kazanma amacıyla [üçüncü taraflara](#) aktarılmasını veya veri alışverişini ifade eder.
 - Kullanıcılar tarafından başlatılan kişisel ve hassas kullanıcı verisi aktarımı (ör. kullanıcı, uygulamanın bir özelliğini kullanarak üçüncü bir tarafa dosya aktardığında veya özel amaca yönelik araştırma uygulaması kullandığında) satış olarak değerlendirilmez.

Belirgin Açıklama ve Rıza Şartı

Uygulamanızın, kişisel ve hassas kullanıcı verilerine erişme, verileri toplama, kullanma veya paylaşma süreçleri, söz konusu ürün ya da özelliğin kullanıcılarından makul ölçüde beklenebilecek amaçların dışındaysa (ör. uygulamanız kullanılmıyorken arka planda veri toplanıyorsa) aşağıdaki şartları yerine getirmeniz gerekir:

Belirgin açıklama: Verilere erişme, verileri toplama, kullanma ve paylaşma sürecinizle ilgili bir uygulama içi açıklama sağlamanız gerekir. 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 toplandığını açıklamalıdır;
- Verilerin nasıl kullanılacağı ve/veya paylaşılacağını açıklamalıdır;
- Yalnızca bir gizlilik politikasına veya hizmet şartlarına eklenmemelidir;
- Kişisel ve hassas kullanıcı verilerinin toplanmasıyla ilgisi olmayan diğer açıklamalara dahil edilmemelidir.

Rıza ve çalışma zamanında istenen izinler: Uygulama içi kullanıcı rızası isteklerinin ve çalışma zamanında istenen izinlerin hemen öncesinde bu politika şartına uygun bir uygulama içi açıklama görüntülenmelidir. Uygulamanızın izin isteği:

- Rıza mesajını açık ve net bir şekilde sunmalıdır;
- Kullanıcının onay verdiğini gösteren bir işlem yapmasını (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;
- Otomatik kapanan veya süresi dolan mesajları kullanıcıdan izin almak için kullanmamalıdır ve
- Uygulamanız kişisel ve hassas kullanıcı verilerini toplamaya veya bu verilere erişmeye başlamadan önce kullanıcı tarafından verilmelidir.

AB GDPR kapsamında meşru menfaat gibi başka yasal gerekçelere dayanarak kişisel ve hassas kullanıcı verilerini izinsiz bir şekilde işleyen uygulamalar geçerli tüm yasal şartlara uymalı ve bu politika uyarınca yapılması zorunlu olan uygulama içi açıklamalar da dahil olmak üzere uygun açıklamaları kullanıcılara sunmalıdır.

Politika şartlarına uymak için zorunlu olduğu durumlarda, belirgin açıklamayı oluştururken aşağıdaki örnek biçimi esas almanız önerilir:

- “[Bu uygulama] [şu senaryoda] [“belirtilen özelliği”] sağlayabilmek için [şu türdeki verileri] toplar/aktarır/senkronize eder/depolar.
- *Örnek: “Fitness Funds uygulaması, kapalıyken veya kullanılmadığında dahi fitness takibini etkinleştirmek için konum verilerini toplar ve ayrıca reklamların sunulmasına yardımcı olmak için kullanılır.”*
- *Örnek: “Call Buddy uygulaması, kullanılmadığında dahi kişi bilgilerinin düzenlenmesi için arama kaydı verilerini toplar, okur ve yazar.”*

Uygulamanıza varsayılan olarak kişisel ve hassas kullanıcı verilerini toplamak üzere tasarlanmış bir üçüncü taraf kodu (ör. bir SDK) entegre edilmişse Google Play'den talep aldıktan sonra iki hafta içinde (ya da Google Play'in talebinde belirtilen süre zarfında) uygulamanızın bu politikanın belirgin açıklama ve rıza şartını (üçüncü taraf kodu aracılığıyla veri paylaşımı, erişimi, toplanması veya kullanımı açısından dahil) yerine getirdiğini gösteren yeterli kanıt sunmanız gerekir.

Yaygın görülen ihlallere ilişkin bazı örnekleri aşağıda bulabilirsiniz:

- Cihaz konumu bilgilerini toplayan ancak hangi özelliğin bu verileri kullandığı hakkında bilgi veren ve/veya uygulamanın arka planda kullanıldığını gösteren bir öne çıkan açıklaması olmayan uygulama.
- Verilerin ne için kullanıldığının belirtildiği belirgin açıklamadan önce verilere erişmek isteyen ve çalışma zamanında istenen izne sahip uygulama.
- Bir kullanıcının yüklü uygulama envanterine erişen ve bu verileri yukarıdaki Gizlilik Politikası, veri işleme, belirgin 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, Öne Çıkan Açıklama ve Rıza şartlarına tabi kişisel veya hassas veri olarak ele almayan bir uygulama.
- Kullanıcının ekranını kaydeden ve bu verileri bu politikaya tabi kişisel veya hassas veri olarak ele almayan bir uygulama.
- **Cihaz konumu** bilgilerini toplayan ve yukarıdaki şartlara uygun şekilde kullanımını açık bir şekilde paylaşmayan ve kullanıcının rızasını almayan bir uygulama.
- Takip etme, araştırma veya pazarlama gibi amaçlarla uygulamanın arka planında kısıtlı izinleri kullanan ve yukarıdaki şartlara uygun şekilde kullanımını açık bir şekilde paylaşmayan ve kullanıcının rızasını almayan bir uygulama.
- Kişisel ve hassas kullanıcı verilerini toplayan bir SDK içeren ancak bu verileri bu Kullanıcı Verileri Politikası'na, erişim, veri işlemenin yanı sıra (izin verilmeyen satış dahil) belirgin açıklama ve rıza şartlarına tabi olarak değerlendirmeyen bir uygulama.

Belirgin açıklama ve rıza şartı hakkında daha fazla bilgi için bu [makaleyi](#) inceleyin.

Kişisel ve Hassas Verilere Erişim Kısıtlamaları

Yukarıdaki şartlara ek olarak, aşağıdaki tabloda belirli etkinliklere ilişkin şartlar açıklanmaktadır.

Etkinlik	Gereksinim
Uygulamanız finans veya ödeme bilgilerini ya da resmi kimlik numaralarını işliyor	Uygulamanız finansal işlemler, ödeme işlemleri veya resmi kimlik numaralarıyla ilgili kişisel ve hassas kullanıcı verilerini hiçbir zaman herkese açık bir şekilde açıklamamalıdır.
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.
Uygulamanız çocukları hedefliyor	Uygulamanız, çocuklara yönelik hizmetlerde kullanımı onaylanmamış SDK'lar içermemelidir. Politika dilinin tamamı ve şartları için Çocuklar ve Aileler için Uygulama Tasarlama başlığını inceleyin.
Uygulamanız kalıcı cihaz tanımlayıcıları topluyor veya bunlara bağlantı veriyor (ör. IMEI, IMSI, SIM Seri Numarası vb.)	Kalıcı cihaz tanımlayıcıları, aşağıdaki amaçlar dışında diğer kişisel ve hassas kullanıcı verilerine veya sıfırlanabilir cihaz tanımlayıcılarına bağlanamaz: - SIM kimliğine (ör. operatörün hesabına bağlı kablosuz arama) bağlı telefon işlevleri ve - Cihaz sahibi modunu kullanan kurumsal cihaz yönetim uygulamaları. Bu kullanımlar, Kullanıcı Verileri Politikası 'nda belirtildiği gibi kullanıcılara belirgin bir şekilde açıklanmalıdır. Alternatif benzersiz tanımlayıcılar için lütfen bu kaynağa bakın. Android Reklam Kimliği ile ilgili ek yönergeler hakkında bilgi edinmek için lütfen Reklam politikasını okuyun.

Veri güvenliği bölümü

Tüm geliştiriciler, her uygulama için kullanıcı verilerinin nasıl toplandığını, kullanıldığını ve paylaşıldığını açıklayan Veri Güvenliği bölümü hazırlamalıdır. Bu açıklamadaki bilgilerin kolay anlaşılabilir ve doğru olması gerekir. Etiketin doğruluğu ve bu bilgilerin güncel tutulması geliştiricinin sorumluluğundadır. Veri Güvenliği bölümü, uygulamanın gizlilik politikasında yapılan açıklamaların ilgili kısımlarıyla tutarlı olmalıdır.

Veri Güvenliği bölümünü tamamlamayla ilgili daha fazla bilgi için lütfen [bu makaleye](#) bakın.

Gizlilik Politikası

Tüm uygulamalar Play Console'da belirtilen alanda bir gizlilik politikası bağlantısı, uygulamanın kendi içinde de bir gizlilik politikası bağlantısı veya metni yayınlamalıdır. Gizlilik politikası, uygulama içi açıklamalarla birlikte uygulamanızın kullanıcı verilerine nasıl eriştiğini, bu verileri nasıl topladığını, kullandığını ve paylaştığını eksiksiz bir şekilde açıklamalıdır. Bu tür kullanıcı verilerine Veri Gizliliği bölümünde açıklanan veriler dahildir ancak bunlarla sınırlı değildir. Açıklama şunları içermelidir:

- Geliştirici bilgileri ve gizlilikle ilgili konularda irtibat kişisi veya sorguları göndermek için kullanılabilen bir mekanizma
- Uygulamanızın ne tür kişisel veya hassas kullanıcı verilerini topladığı, kullandığı, paylaştığı; ayrıca kişisel veya hassas kullanıcı verilerinin paylaşıldığı tüm tarafların açıklaması
- Kişisel ve hassas kullanıcı verileri için güvenli veri işleme süreçleri

- Geliştiricinin veri saklama ve silme politikası
- Anlaşılır bir gizlilik politikası ibaresi (örneğin, başlıkta "gizlilik politikası" ifadesi)

Uygulamanın Google Play girişinde adı geçen tüzel kişi (örneğin geliştirici, şirket), gizlilik politikasında yer almalı veya uygulamanın adı gizlilik politikasında belirtilmelidir. Hiçbir kişisel ve hassas kullanıcı verisine erişmeyen uygulamalar yine de gizlilik politikası sağlamalıdır.

Lütfen gizlilik politikanızın çalışan, herkesin erişimine açık ve coğrafi sınıra tabi olmayan bir URL'de bulunduğundan (PDF kabul edilmez.) ve düzenlenebilir olmadığından emin olun.

Hesap Silme Şartı

Kullanıcılarınıza uygulamanızın içinde hesap oluşturma hakkı tanıyorsanız hesaplarını silme isteğinde bulunma hakkı da tanımanız gerekir. Kullanıcılar, uygulama hesabı silme işlemini uygulamanızın içinden ve dışından (ör. web sitenizden) kolayca başlatabilmelidir. Bu web kaynağının bağlantısı, Play Console'da belirtilen URL form alanına girilmelidir.

Bir kullanıcının isteği üzerine uygulama hesabını sildiğinizde, o uygulama hesabıyla ilişkilendirilen kullanıcı verilerini de silmeniz gerekir. Uygulama hesabının geçici olarak devre dışı bırakılması veya "dondurulması", hesabın silinmesi olarak kabul edilmez. Güvenlik, sahtekarlık önleme veya tüzüklere uygunluk gibi meşru gerekçelerle belirli verileri saklamanız gerekiyorsa kullanıcıları veri saklama yöntemleriniz hakkında açıkça bilgilendirmeniz (ör. gizlilik politikanızda) gerekir.

Hesap silmeyle ilgili politika şartları hakkında daha fazla bilgi için [bu Yardım Merkezi makalesini](#) inceleyebilirsiniz. Veri Güvenliği Formunuzu güncelleme hakkında ek bilgi için [bu makaleyi](#) okuyabilirsiniz.

Uygulama Grubu Kimliğinin Kullanımı

Android'de, analizler ve sahtekarlığı önleme gibi önemli kullanım alanlarını desteklemek üzere yeni bir kimlik kullanımı başlatılacak. Bu kimliğin kullanımıyla ilgili şartlar aşağıdadır.

- **Kullanım:** Uygulama grubu kimliği, reklam kişiselleştirme ve reklam ölçümü gibi amaçlarla kullanılamaz.
- **Kimliği tanımlayabilecek bilgiler veya diğer tanımlayıcılarla olan ilişki:** Uygulama grubu kimliği, herhangi bir Android kimliğine (ör. AAID) veya reklam amacıyla herhangi bir kişisel ve hassas veriye bağlanamaz.
- **Şeffaflık ve kullanıcı izni:** Uygulama grubu kimliğinin toplanması, kullanılması ve bu şartlara bağlılık, gizlilik politikanız da dahil olmak üzere yasal anlamda yeterli düzeyde bir gizlilik bildirimi aracılığıyla kullanıcılara açıklanmalıdır. Gerektiğinde kullanıcılardan yasal olarak geçerli izin almanız gerekir. Gizlilik standartlarımız hakkında daha fazla bilgi edinmek için lütfen [Kullanıcı Verileri politikamıza](#) bakın.

EU-U.S., Swiss Privacy Shield (AB-ABD, İsviçre Gizlilik Kalkanı)

Avrupa Birliği veya İsviçre kaynaklı olup bir bireyin kimliğini doğrudan ya da 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 kořullara uygunluęunuzu d zenli olarak izlemelisiniz. Bu řartları yerine getiremezseniz (ya da bu řartları yerine getiremeyeceęinize dair  nemli bir risk varsa) hemen data-protection-office@google.com adresine e-posta g ndererek durumu bize bildirmeniz ve derhal ya AB Kiřisel Bilgilerini iřlemeyi durdurmanız ya da yeterli koruma seviyesini saęlamak i in makul ve uygun adımları atmanız gerekir.

16 Temmuz 2020 tarihinden itibaren artık Avrupa Ekonomik Alanı veya Birleřik Krallık'tan ABD'ye veri aktarımında EU-U.S. Privacy Shield'e (AB-ABD Gizlilik Kalkanı) itimat etmiyoruz. ([Daha Fazla Bilgi](#).) Daha fazla bilgi i in DDA'nın 9. B l m ne bakın.

Hassas Bilgilere Eriřen İzinler ve API'ler

İzin talepleri ve hassas bilgilere eriřimi olan API'ler, kullanıcılar a ısından anlamlı olmalıdır. Yalnızca Google Play giriřinizde tanıtılan mevcut  zelliklerin veya hizmetlerin uygulamanızda kullanılabilmesi i in gereken izinleri ve hassas bilgilere eriřimi olan API'leri isteyebilirsiniz. A ıklanmayan, hen z uygulanmamıř veya izin verilmeyen  zellikler ya da ama lar i in kullanıcı veya cihaz verilerine eriřim saęlayan izinleri ya da hassas bilgilere eriřimi olan API'leri kullanamazsınız. İzinler veya hassas bilgilere eriřimi olan API'ler  zerinden eriřilen kiřisel veya hassas veriler hi bir zaman satılamaz ya da satıřı kolaylařtıracak bir ama  doęrultusunda paylařılamaz.

İzinleri ve hassas bilgilere eriřimi olan API'leri, verilere eriřmek i in gereklilik olduęu anda (sırası geldięinde) isteyerek kullanıcıların, uygulamanızın neden izin istedięini anlamalarını saęlayın. Verileri yalnızca kullanıcının izin verdięi ama lar i in kullanın. Verileri daha sonra bařka ama lar i in kullanmak isterseniz, kullanıcılara bunu sormalı ve ek kullanımları kabul ettiklerinden emin olmalısınız.

Kısıtlanmış İzinler

Yukarıdakilere ek olarak, kısıtlı izinler [Tehlikeli](#) , [ zel](#) , [İmza](#) olarak ifade edilen veya ařaęıda belirtilen izinlerdir. Bu izinler, ařaęıda a ıklanan ek řartlara ve kısıtlamalara tabidir:

- Kısıtlanmış İzinler  zerinden eriřilen kullanıcı veya cihaz verileri, kiřisel ve hassas kullanıcı verileri olarak kabul edilir. [Kullanıcı Verileri Politikası](#) 'nın řartları ge erlidir.
- Kullanıcılar Kısıtlı İzin isteęini reddederse kararlarına saygı duyun. Kullanıcılar ayrıca kritik olmayan izinlere rıza g stermeleri i in manip le edilemez veya zorlanamaz. Hassas izinlere eriřim hakkı vermeyen kullanıcıların uygulamanızı kullanabilmesini saęlamak i in makul  l  de  aba g stermeniz gerekir ( rneęin, Arama Kayıtları'na eriřimi kısıtlayan kullanıcıların manuel olarak telefon numarası girmelerine izin vermek).
- İzinlerin Google Play [K t  Ama lı Yazılım Politikası](#) 'na ([ st D zey Ayrıcalıkları K t ye Kullanma](#) dahil) aykırı řekilde kullanılması a ık a yasaktır.

Bazı Kısıtlı İzinler ařaęıda a ıklandığı řekilde ek řartlara tabi olabilir. Bu kısıtlamaların amacı kullanıcının gizlilięini teminat altına almaktır. Uygulamaların olduk a etkileyici veya  ok  nemli bir  zellik sunması ve bu  zellięi saęlamanın bařka alternatif y ntemi olmaması gibi  ok nadir durumlarda řartlarda sınırlı istisnalar yapabiliriz. Teklif edilen istisnaları deęerlendirerek kullanıcıların gizlilięi veya g venlięi  zerinde olası etkileri olup olmadıęına bakarız.

SMS ve Arama Kaydı İzinleri

SMS ve Arama Kaydı İzinleri, [Kiřisel ve Hassas Bilgiler](#) politikasına ve ařaęıdaki kısıtlamalara tabi kiřisel ve hassas kullanıcı verileri olarak deęerlendirilir:

Kısıtlı İzinler	Gereksinim
Arama Kaydı izin grubu (�r. READ_CALL_LOG, WRITE_CALL_LOG, PROCESS_OUTGOING_CALLS)	Cihazda etkin bir řekilde varsayılan Telefon veya Asistan iřleyici olarak kayıtlı olmalıdır.
SMS izin grubu (�r. READ_SMS, SEND_SMS, WRITE_SMS, RECEIVE_SMS, RECEIVE_WAP_PUSH, RECEIVE_MMS)	Cihazda etkin bir řekilde varsayılan SMS veya Asistan iřleyici 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 özellikleri 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](#) politikası, [Arka Planda Konum politikası](#) 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 iznili 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.

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.

Politika şartları hakkında daha fazla bilgiyi bu [yardım makalesinde](#) bulabilirsiniz.

Tüm Dosyalara Erişim İzni

Bir kullanıcının cihazındaki dosyalar ve dizin 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 veya sonraki bir sürümü çalıştıran Android cihazlarda, paylaşılan depolama alanındaki erişimi yönetmek için [MANAGE_EXTERNAL_STORAGE](#) izni gerekecektir. 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.

Paket (Uygulama) Görünürlüğü İzni

Bir cihazdan sorgulanan yüklü uygulama envanteri, [Kişisel ve Hassas Bilgiler](#) politikasının yanı sıra aşağıdaki şartlara tabi kişisel ve hassas kullanıcı verileri olarak değerlendirilir:

Temel amacı cihazdaki diğer uygulamaları başlatmak, aramak veya diğer uygulamalarla birlikte çalışmak olan uygulamalar, diğer uygulamaları aşağıda açıklandığı şekilde kapsama uygun olarak görme yeteneğine sahip olmalıdır:

- **Genel uygulama görünürlüğü:** Genel görünürlük, bir uygulamanın cihazdaki yüklü uygulamaları ("paketler") kapsamlı (veya "genel") bir şekilde görebilmesidir.
 - [API düzeyi 30 veya sonrasını](#) hedefleyen uygulamaların, [QUERY_ALL_PACKAGES](#) izni üzerinden yüklü uygulamaları görebilmesi; uygulamanın çalışabilmesi için cihazdaki tüm uygulamaları bilmesi ve/veya onlarla birlikte çalışmasının gerektiği belirli kullanım alanlarıyla kısıtlanmıştır.
 - Uygulamanız daha çok [hedeflenmiş kapsamdaki paket görünürlüğü bildirimi](#) ile çalışabiliyorsa (ör. genel görünürlük talep etmek yerine belirli paketleri sorgulama ve etkileşim kurma) [QUERY_ALL_PACKAGES](#) iznini kullanamazsınız.
 - [QUERY_ALL_PACKAGES](#) izniyle ilişkili genel görünürlük düzeyini tahmin etmek için alternatif yöntemler kullanmak da, kullanıcının gördüğü temel uygulama işlevleri ve bu yöntemle keşfedilen uygulamalarla birlikte çalışmayla sınırlıdır.
 - [QUERY_ALL_PACKAGES](#) için izin verilen kullanım alanları hakkında bilgiyi bu [Yardım Merkezi makalesinde](#) bulabilirsiniz.
- **Sınırlı uygulama görünürlüğü:** Sınırlı görünürlük, bir uygulamanın "genel" yöntemler yerine daha hedefe yönelik yöntemlerle (ör. uygulamanızın manifest bildirimini karşılayan belirli uygulamaları sorgulamak gibi) spesifik uygulamaları sorgulayarak verilere erişimini en aza indirdiği durumdur. Uygulamanızın politikaya uygun bir şekilde birlikte çalışabildiği veya uygulamaları yönetebildiği durumlarda bu uygulamaları sorgulamak için bu yöntemi kullanın.
- Bir cihazda yüklü uygulama envanterinin görünürlüğü, kullanıcıların uygulamanızda eriştikleri temel amaç veya temel işlevlerle doğrudan alakalı olmalıdır.

Play'de dağıtılan uygulamaların sorgulanmasıyla elde edilen uygulama envanteri verileri, hiçbir zaman analiz veya reklamlardan para kazanma amacıyla satılamaz veya paylaşılamaz.

Accessibility API

Accessibility API'nin kullanılamayacağı durumlar:

- Ebeveyn denetimi uygulaması aracılığıyla bir ebeveyn veya vasi tarafından ya da kurumsal yönetim yazılımı aracılığıyla yetkili yöneticiler tarafından yetki verilmediği sürece izinsiz şekilde kullanıcı ayarlarının değiştirilmesi veya kullanıcıların herhangi bir uygulama ya da hizmeti devre dışı bırakmasının veya kaldırmasının engellenmesi;
- Android içerisindeki yerleşik gizlilik denetimleri ve bildirimlerine geçici çözüm bulunması veya
- Kullanıcı arayüzünün, aldatıcı veya Play Geliştirici Politikaları'nı ihlal edecek şekilde değiştirilmesi ya da kullanılması.

Accessibility API, aramalarda uzaktan ses kaydı için tasarlanmamış olup bu amaçla talep edilemez.

Accessibility API'nin kullanımı Google Play girişinde belgelenmelidir.

IsAccessibilityTool ile ilgili yönergeler

Engelli bireyleri doğrudan desteklemeyi amaçlayan temel işlevlere sahip uygulamalar, kendilerini uygun ve açık bir şekilde erişilebilirlik uygulaması olarak tanımlamak için **IsAccessibilityTool**'u kullanabilir.

IsAccessibilityTool'u kullanmaya uygun olmayan uygulamalar, erişilebilirlikle ilgili işlevin kullanıcılar açısından açık olmaması nedeniyle bu işareti kullanmamalı ve [Kullanıcı Verileri politikasında](#) belirtildiği üzere, belirgin şekilde açıklama ve izin şartlarını karşılamalıdır. Daha fazla bilgi için [AccessibilityService API](#) yardım merkezi makalesine göz atın.

Uygulamalar, istenilen işlevselliğe ulaşmak için mümkün olduğunda Accessibility API yerine daha dar kapsamlı [API'ler ve izinler](#) kullanmalıdır.

Paket Yükleme İzni İsteme

[REQUEST_INSTALL_PACKAGES](#) izni, uygulamaların uygulama paketi yükleme isteğinde bulunmasını sağlar. Bu izni kullanabilmek için uygulamanızın temel işlevi şunları içermelidir:

- Uygulama paketi gönderme veya alma ve
- Uygulama paketi yüklemenin kullanıcılar tarafından başlatılabilmesini sağlama

İzin verilen işlevler şunlardır:

- Web'de gezinme veya arama yapma
- Ekleri destekleyen iletişim hizmetleri
- Dosya paylaşımı, aktarımı veya yönetimi
- Kurumsal cihaz yönetimi
- Yedekleme ve geri yükleme
- Cihaz Taşıma/Telefon Aktarma
- Telefonu giyilebilir veya IoT cihazla senkronize eden tamamlayıcı uygulama (örneğin, akıllı saat veya akıllı TV)

Temel işlev, uygulamanın asıl amacı olarak tanımlanır. Temel işlevin ve bunu oluşturan tüm temel özelliklerin uygulamanın açıklamasında belirgin bir şekilde yer alması ve tanıtılması gerekir.

[REQUEST_INSTALL_PACKAGES](#) izni, cihaz yönetimi amacıyla olmadığı sürece öge dosyasında diğer APK'ları paket haline getirmek, kendi kendine güncellemeler ve değişiklikler yapmak için kullanılamaz. Tüm güncelleme veya paket yükleme işlemleri Google Play'in [Cihazları ve Ağı Kötüye Kullanma Politikası](#)'na uygun olarak kullanıcı tarafından başlatılmalı ve yürütülmelidir.

Android Health Connect İzinleri

[Health Connect](#), sağlık ve fitness uygulamalarının cihaz üzerindeki aynı verileri, birleştirilmiş bir ekosistemde saklayıp paylaşmasına olanak tanıyan bir Android platformudur. Ayrıca hangi uygulamaların, sağlık kayıtları da dahil olmak üzere sağlık ve fitness verilerini okuyup yazabileceğinin tek bir yerden kontrol edilmesini sağlar. Sağlık kayıtları, sağlık hizmeti sağlayıcılarından veya kurumlarından ya da desteklenen üçüncü taraf sağlık platformları aracılığıyla elde edilen tıbbi geçmiş, teşhis, tedavi, ilaç, tahlil sonucu ve diğer klinik verileri içerebilir.

Health Connect, adım sayısından vücut sıcaklığına ve sağlık kaydı verilerine kadar [çeşitli veri türlerinin](#) okunup yazılmasını destekler.

Health Connect izinleri üzerinden erişilen veriler, kişisel ve hassas kullanıcı verisi olarak değerlendirilmekle birlikte [Kullanıcı Verileri Politikası](#)'na tabidir. Uygulamanız sağlık uygulaması olarak kabul ediliyorsa ya da sağlıkla alakalı özellikler içeriyor ve Health Connect verileri de dahil olmak üzere sağlık verilerine erişiyorsa [Sağlık Uygulamaları Politikası](#)'na da uymalıdır.

Health Connect'i nasıl kullanmaya başlayacağınızı öğrenmek için bu [Android geliştirici kılavuzunu](#) inceleyebilirsiniz. Health Connect veri türlerine ve diğer sık sorulan sorulara erişim isteğinde bulunmak için [Health Connect politika koşullarıyla ilgili sık sorulan sorular](#) sayfasına göz atın.

Google Play aracılığıyla dağıtılan uygulamaların Health Connect'te veri okuyabilmesi ve/veya yazabilmesi için aşağıdaki politika koşullarını karşılaması gerekir.

Health Connect Erişiminin ve Kullanımının Uygunluğu

Health Connect yalnızca bu politikada belirtilen onaylı kullanım alanlarına uygun şekilde kullanılmalıdır. Bu kullanım, geçerli politikaların yanı sıra hükümler ve koşullara uymalıdır. Yani yalnızca uygulamanız veya hizmetinizin onaylanan kullanım alanlarından birine uyması halinde söz konusu izinlere erişim isteyebilirsiniz.

Onaylanan kullanım alanları arasında fitness ve sağlıklı yaşam, ödüller, fitness koçluğu, kurumsal sağlıklı yaşam, tıbbi bakım, sağlık araştırması ve oyunlar yer alır. Bu kullanım alanlarına erişim hakkı tanınan uygulamalar, kullanım alanlarını, açıklanmayan veya izin verilmeyen amaçlarla kullanamaz.

Yalnızca kullanıcıların sağlık ve fitness durumuna katkı sağlamak için tasarlanmış bir veya daha fazla özelliğe sahip uygulama ya da hizmetlerin Health Connect izinlerine erişim isteğinde bulunmasına izin verilir. Bunlardan bazıları:

- Kullanıcının fiziksel aktivite, uyku, ruh sağlığı ve beslenme bilgilerini, sağlık ölçümlerini, vücut ölçülerini, sağlık kayıtlarını ve/veya sağlıkla ya da fitness ile ilgili bilgi ve ölçümlerini **doğrudan kaydetmesine, raporlamasına, takip etmesine ve/veya analiz etmesine** imkan veren uygulama veya hizmetler
- Kullanıcıların **fiziksel aktivite, uyku, ruh sağlığı ve beslenme bilgilerini, sağlık ölçümlerini, vücut ölçülerini, sağlık kayıtlarını** ve/veya sağlıkla ya da fitness ile ilgili bilgi ve ölçümlerini cihazlarında saklamalarına ve bu kullanım alanlarına uygun olup cihaz üzerinde bulunan diğer uygulamalarla verilerini paylaşmalarına imkan veren uygulama veya hizmetler
- Kronik rahatsızlıkların, tıbbi tedavilerin veya bakım desteğinin kullanıcılar tarafından yönetilmesini sağlayan uygulamalar ya da hizmetler

Health Connect erişimi; aşağıdaki amaçlara yönelik kullanımlar dahil olmak üzere bu politikayı veya diğer geçerli Health Connect hükümlerini ve koşullarını ya da politikalarını ihlal edecek şekilde kullanılamaz:

- Health Connect; Health Connect'in kullanımı veya Health Connect'te yaşanacak bir hata sonucunda ölüm, kişisel yaralanma, başka kişilere zarar verme ya da çevreye veya mala yönelik zarar oluşma olasılığı olan uygulamaların, ortamların ya da faaliyetlerin (örneğin, hava trafik kontrolü, yaşam destek veya silah sistemlerinin veya nükleer tesislerin kurulması ya da işletilmesi) geliştirilmesinde kullanılmamalı veya bunlara eklenmemelidir.
- Health Connect üzerinden edinilen verilere gözetimsiz uygulamalar kullanılarak erişilmemelidir. Uygulamalar uygulama tepsisinde, cihaz uygulama ayarlarında, bildirim simgelerinde ve benzeri yerlerde net bir şekilde tanımlayıcı simge görüntülemelidir.
- Health Connect, uyumsuz cihazlar veya platformlar arasında veri senkronizasyonu yapan uygulamalarla kullanılmamalıdır.
- Health Connect yalnızca çocukları hedefleyen uygulamalara, hizmetlere veya özelliklere bağlanmak için kullanılmamalıdır.
- Health Connect'i kullanan uygulamaları veya sistemleri yetkisiz ya da yasa dışı erişime, kullanıma, saldırıya, kayba, bozulmaya veya izinsiz paylaşımına karşı korumak için makul ve uygun önlemler alın.

Ayrıca Health Connect'i ve Health Connect'ten alınan verileri kullanma amacınız doğrultusunda geçerli olabilecek tüm yönetmeliklere ve yasal koşullara uyulmasını sağlama yükümlülüğü size aittir. Örneğin, Sağlık Sigortası Taşınabilirlik ve Sorumluluk Yasası'na (HIPAA) tabi bir tüzel kişi veya ticari ortaklarınız Health Connect'teki bilgilere erişiminiz ve bu bilgileri kullanımınızla ilgili geçerli şartlara uymanız gerekir. AB'deki kullanıcılar için Genel Veri Koruma Yönetmeliği'ne (GDPR) tabi bir geliştiriciyseniz benzer şekilde GDPR kapsamındaki yükümlülüklerinizi yerine getirmeniz gerekir. Bu yasalar ve yönetmelikler uyarınca, işleme faaliyetlerinizin bir parçası olan tüzel kişilerle veri paylaşmadan önce ek sözleşmeler (ör. Ticari Ortaklık Sözleşmesi veya Veri İşleme Sözleşmesi) yapmanız gerekebilir. Faaliyetleri için bu tür sözleşmelerin gerekli olup olmadığını belirlemek de uygulama geliştiricilerin sorumluluğundadır.

Geliştiriciler, talep edilmesi halinde Google'a bu sözleşmeler veya uygunlukla ilgili kanıt sunmak zorundadır.

Belirli Google ürünleri veya hizmetleri için Google tarafından sağlanan etiketlerde ya da bilgilerde açıkça belirtilmediği sürece Google; Health Connect'te bulunan hiçbir verinin özellikle araştırma, sağlık veya medikal alanında olmak üzere hiçbir amaca yönelik olarak kullanımını desteklemez ya da doğruluğunu garanti etmez. Google, Health Connect üzerinden edinilen verilerin kullanılmasıyla ilgili tüm sorumlulukları reddeder.

Sınırlı Kullanım

Health Connect kullanılırken veri erişimi ve kullanımı bazı sınırlamalara tabidir:

- Veri kullanımı, uygun kullanım alanının veya uygulamanın kullanıcı arayüzünde görünen özelliklerin sağlanması ya da iyileştirilmesiyle sınırlı olmalıdır.
- Kullanıcı verileri yalnızca açık kullanıcı izni olduğunda, güvenlik nedeniyle (ör. kötüye kullanımı araştırmak için), geçerli yasalara veya tüzüklere uymak için ya da birleşme/satın alma kapsamında üçüncü taraflara aktarılabilir.
- İnsanlar kullanıcı verilerine yalnızca açıkça kullanıcı izni alındığında, güvenlik nedeniyle, yasalara uymak için veya yasal koşullar kapsamında dahili işlemler için toplandığında erişebilirler. Aksi halde kullanıcı verilerine insan erişimi kısıtlanmıştır.
- **Aşağıdakiler dahil olmak üzere diğer tüm durumlarda Health Connect verilerinin aktarılması, kullanılması ve satılması yasaktır:**
 - Reklamcılık platformu, veri aracısı ya da bilgi satıcısı gibi üçüncü taraflara kullanıcı verilerinin aktarılması veya satılması;
 - Kullanıcı verilerinin, kişiselleştirilmiş veya ilgi alanına dayalı reklamlar dahil olmak üzere reklam yayınlamak amacıyla aktarılması, satılması ya da kullanılması;
 - Kullanıcı verilerinin, kredibilite tespiti veya kredi verme amacıyla aktarılması, satılması ya da kullanılması;
 - Kullanıcı verilerinin tıbbi cihaz olarak nitelenebilen ürün ya da hizmetlere aktarılması, satılması veya bunlarla kullanılması (tıbbi cihaz uygulamasının geçerli tüm düzenlemelere uyduğu, Health Connect verilerini kullanmak için ilgili düzenleyici kurumlardan (ör. ABD Gıda ve İlaç İdaresi (FDA)) gerekli izinleri ve onayları aldığı ve kullanıcının bu kullanıma açıkça izin verdiği durumlar hariç);
 - Kullanıcı tarafından başlatılmadığı ve HIPAA yönetmeliklerine uygun olmadığı sürece, Korunan Sağlık Bilgileri (HIPAA tarafından tanımlandığı şekilde) ile ilişkili herhangi bir amaç doğrultusunda ya da herhangi bir şekilde kullanıcı verilerinin aktarılması, satılması veya kullanılması

Minimum Kapsam

Yalnızca ürününüzün özelliklerinin veya hizmetlerinin kullanımı için gerekli olan izinlere erişim isteğinde bulunmalısınız. Bu tür erişim istekleri spesifik olmalı ve yalnızca gereken verileri kapsamalıdır.

Şeffaf ve Doğru Bilgilendirme ve Kontrol

Health Connect'in işlediği sağlık ve fitness verileri, kişisel ve hassas bilgiler içerir. Geliştiriciler, kapsamlı bir gizlilik politikası oluşturarak veri uygulamaları hakkında anlaşılır ve erişilebilir açıklamalar sağlamalıdır. Bu açıklamalarda şu bilgiler yer almalıdır:

- Kullanıcı verilerine erişim izni isteyen uygulama veya hizmetin doğru şekilde yansıtılan kimliği
- Erişilen, istenen ve/veya toplanan veri türleriyle ilgili anlaşılır ve doğru bilgiler. Veriler, uygulamanızda sunulan bir öneriyle veya kullanıcılara yönelik bir özelliklerle alakalı olmalıdır.
- Verilerin nasıl kullanılacağı ve/veya paylaşılabileceği hakkında açıklama: Bir nedenle talep ettiğiniz verinin başka bir amaç için de kullanılacağı durumlarda tüm kullanım alanlarını açıklamamız gerekir.
- Kullanıcıların uygulamadaki verilerini nasıl yönetebileceğini ve silebileceğini, ayrıca hesap devre dışı bırakıldığında ve/veya silindiğinde verilere ne olacağını açıklayan kullanıcı yardım belgeleri

- Modern kriptografi kullanarak iletme (örneğin, HTTPS üzerinden) de dahil olmak üzere tüm kişisel ve hassas kullanıcı verilerini güvenli bir şekilde işlemeye ilgili bilgiler

Health Connect'e bağlanan uygulamaların tabi olduğu koşullar hakkında daha fazla bilgi için lütfen bu [Yardım Merkezi](#) makalesini inceleyin.

VPN Hizmeti

[VpnService](#) , uygulamaların kendi VPN çözümlerini oluşturup geliştirmesine olanak tanıyan bir temel sınıftır. Yalnızca VpnService'i kullanan ve temel işlevi VPN olan uygulamalar uzaktaki bir sunucuya cihaz seviyesinde güvenli bir tünel oluşturabilir. Temel işlevi için uzaktaki bir sunucuya ihtiyaç duyan uygulamalar istisna kapsamında yer alır. Örneğin:

- Ebeveyn denetimi ve kurumsal yönetim uygulamaları
- Uygulama kullanımını izleyen uygulamalar
- Cihaz güvenliği uygulamaları (ör. virüsten korunma, mobil cihaz yönetimi, güvenlik duvarı)
- Ağla alakalı araçlar (ör. uzaktan erişim)
- Web'de gezinme uygulamaları
- Telefon ve bağlantı hizmetlerini sunmak için VPN işlevleri kullanılmasını gerektiren operatör uygulamaları

VpnService şu amaçlar için kullanılamaz:

- Öne çıkan açıklama ve izin olmadan kişisel ve hassas kullanıcı verilerini toplama
- Para kazanmak için bir cihazdaki diğer uygulamaların kullanıcı trafiğini yönlendirme veya manipüle etme (ör. kullanıcının ülkesi dışında bir ülke üzerinden reklam trafiğini yönlendirme)

VpnService'i kullanan uygulamalar:

- VpnService'in kullanımını Google Play girişinde belirtmelidir ve
- Verileri cihazdan VPN tünelinin son noktasına kadar şifrelemelidir.
- [Reklam Sahtekarlığı](#) , [İzinler](#) ve [Kötü Amaçlı Yazılım](#) politikaları da dahil olmak üzere tüm [Geliştirici Program Politikaları](#) 'na uymalıdır.

Tam Alarm İzni

Android 13 (hedef API düzeyi 33) sürümünden itibaren uygulamalarda [tam alarm işlevine](#) erişim sağlayacak USE_EXACT_ALARM adlı yeni bir izin kullanıma sunulacaktır.

USE_EXACT_ALARM kısıtlı bir izindir ve yalnızca temel işlevleri gereği tam alarm iznini kullanması gereken uygulamalar bu izni beyan etmelidir. Bu kısıtlı izni talep eden uygulamalar incelemeye tabi tutulur ve kabul edilebilir kullanım alanı ölçütlerini karşılamamaları halinde Google Play'de yayınlanmalarına izin verilmez.

Tam Alarm İzni için kabul edilebilir kullanım alanları

Yalnızca uygulamanızın kullanıcılara yönelik temel işlevi aşağıdakiler gibi tam olarak zamanlanmış işlemler gerektiriyorsa USE_EXACT_ALARM işlevini kullanmalısınız:

- Uygulama bir alarm veya zamanlayıcı uygulamasıdır.
- Uygulama, etkinlik bildirimleri gösteren bir takvim uygulamasıdır.

Tam alarm işlevini yukarıdakilerin dışında bir alanda kullanıyorsanız alternatif olarak SCHEDULE_EXACT_ALARM iznini kullanma seçeneğini değerlendirmelisiniz.

Tam alarm işlevi hakkında daha fazla bilgi için lütfen bu [geliştirici kılavuzuna](#) bakın.

Tam ekran intent izni

[USE_FULL_SCREEN_INTENT](#) , Android 14 (API hedef düzeyi 34) ve sonraki sürümleri hedefleyen uygulamalar için [özel uygulama erişim iznidir](#) . Bir uygulamanın otomatik olarak

USE_FULL_SCREEN_INTENT iznini kullanabilmesi için temel işlevi, yüksek öncelikli bildirim gerektiren aşağıdaki kategorilerden birine girmelidir:

- Alarm kurma
- Telefon veya görüntülü görüşme araması alma

Bu izni talep eden uygulamalar incelemeye tabi tutulur ve yukarıdaki ölçütleri karşılamayanlar bu izni otomatik olarak kullanamaz. Bu durumda, uygulamaların USE_FULL_SCREEN_INTENT için kullanıcıdan izin istemesi gerekir.

USE_FULL_SCREEN_INTENT izninin her türlü kullanımının [İstenmeyen Mobil Yazılım, Cihazları ve Ağ Kötüye Kullanma](#) ve [Reklam](#) Politikamız da dahil olmak üzere tüm [Google Play Geliştirici Politikalarına](#) uyması gerektiğini hatırlatırız. Tam ekran intent bildirimleri, kullanıcının cihazına yetkisiz bir şekilde müdahale edemez, zarar veremez, erişemez veya çalışmasını kesintiye uğratamaz. Ayrıca uygulamalar diğer uygulamalara müdahale etmemeli veya cihazın kullanılabilirliğini engellememelidir.

USE_FULL_SCREEN_INTENT izni hakkında daha fazla bilgiyi [Yardım Merkezimizde](#) bulabilirsiniz.

Cihazları ve Ağ 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 veya Android API'lerine dolaylı erişimi olan (bir web görünümündeki veya tarayıcıdaki JavaScript gibi) yorumlayıcıdaki kodlar için geçerli değildir.

Çalıştırma zamanında yüklenen (ör. uygulamaya paket olarak eklenmemiş), yorumlanmış dillere (JavaScript, Python, Lua vb.) sahip uygulamalar veya üçüncü taraf kodları (ör. SDK'lar), Google Play politikalarının olası ihlallerine izin vermemelidir.

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.

Yaygın görülen ihlallere ilişkin bazı örnekleri aşağıda bulabilirsiniz:

Cihazları ve Ağ Kötüye Kullanma Politikası'na dair yaygın ihlal örnekleri:

- 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.
- [İzin verilenler listesine eklenmeye uygun](#) olmayan ve [sistem gücü yönetimini](#) atlatmaya çalışan uygulamalar.
- Üçüncü taraflara proxy hizmetlerini kolaylaştıran uygulamalar bunu yalnızca uygulamanın birincil, kullanıcıya yönelik temel amacı olduğu takdirde yapabilir.
- Google Play dışında bir kaynaktan dex dosyası veya yerel kod gibi yürütülebilir kodlar indiren uygulamalar veya üçüncü taraf kodları (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.
- Güvenilir olmayan web içeriklerini (ör. http:// URL) veya güvenilir olmayan kaynaklardan alınan doğrulanmamış URL'leri (ör. güvenilir olmayan intent'lerle elde edilen URL'ler) yükleyen JavaScript arayüzü eklenmiş web görünümü içeren uygulamalar ya da üçüncü taraf kodları (ör. SDK'lar).
- Kullanıcıları, kullanımı engelleyen reklamlarla veya bildirimlerle etkileşime zorlamak için [tam ekran intent izni](#) kullanan uygulamalar.

Ön Plan Hizmeti Kullanımı

Ön plan hizmeti izni, kullanıcılara yönelik ön plan hizmetlerinin uygun şekilde kullanılmasını sağlar. Android 14 ve sonraki sürümleri hedefleyen uygulamalarda kullanılan her ön plan hizmeti için geçerli bir ön plan hizmeti türü belirtmeniz ve o tür için uygun olan [ön plan hizmeti iznini](#) beyan etmeniz gerekir. Örneğin, uygulamanızın kullanım alanı, haritada coğrafi konumu gerektiriyorsa uygulamanızın manifest dosyasında [FOREGROUND_SERVICE_LOCATION](#) iznini beyan etmeniz gerekir.

Yalnızca aşağıdaki şartları karşılayan uygulamalar ön plan hizmeti iznini beyan edebilir:

- Kullanım, kullanıcı için faydalı ve uygulamanın temel işleviyle alakalı özellikler sağlıyorsa
- Kullanım, kullanıcı tarafından başlatılıyor veya algılanabiliyorsa (örneğin, çalan şarkının sesi, başka cihaza medya içeriği yayınlama, doğru ve net kullanıcı bildirimi, kullanıcının buluta fotoğraf yükleme isteği)
- Kullanım, kullanıcı tarafından sonlandırılabilir veya durdurulabiliyorsa
- Kullanım, olumsuz bir kullanıcı deneyimine yol açmadan veya kullanıcının sunulmasını beklediği özelliğin planlandığı gibi çalışmasını engellemeden sistem tarafından kesintiye uğratılamıyor veya ertelenemiyorsa (örneğin, telefon aramasının hemen başlatılması gerekiyorsa ve arama, sistem tarafından ertelenemiyorsa)
- Kullanım yalnızca görevi tamamlamak için gereken süre boyunca devam ediyorsa

Aşağıdaki ön plan hizmeti kullanım durumları yukarıdaki kriterlerden muaftır:

- [systemExempted](#) veya [shortService](#) ön plan hizmet türleri;
- yalnızca [Play Asset Delivery](#) özellikleri kullanılırken dataSync ön plan hizmet türü

Ön plan hizmetinin kullanımıyla ilgili ayrıntılı bilgiyi [burada](#) bulabilirsiniz.

Kullanıcı Tarafından Başlatılan Veri Aktarımı İşleri

Uygulamaların yalnızca aşağıdaki durumlarda [user-initiated data transfer jobs](#) API'yi kullanmasına izin verilir:

- Kullanım, kullanıcı tarafından başlatılıyorsa
- Kullanım, ağ veri aktarımı görevleri içinse
- Kullanım yalnızca veri aktarımını tamamlamak için gereken süre boyunca devam ediyorsa

User-Initiated Data Transfer API'nin kullanımıyla ilgili ayrıntılı bilgiyi [burada](#) bulabilirsiniz.

Flag Secure İçin Gerekli Şartlar

[FLAG_SECURE](#), kullanıcı arayüzünde hassas veriler bulunduğunu ve uygulama kullanılırken bunların sadece güvenli yüzeylerde görüntülenmesi gerektiğini belirtmek amacıyla uygulamaların kod dosyalarında beyan edilen bir ekran işaretidir. Bu işaret, verilerin ekran görüntülerinde veya güvenli olmayan ekranlarda gösterilmesini engellemek üzere tasarlanmıştır. Geliştiriciler, uygulama içeriğinin yayınlanmaması, görüntülenmemesi veya uygulamanın ya da kullanıcının cihazının dışına aktarılabilmesi gerektiğinde bu işareti beyan ederler.

Güvenlik ve gizlilik nedeniyle, Google Play'de dağıtılan tüm uygulamalar diğer uygulamaların [FLAG_SECURE](#) beyanına saygı göstermelidir. Diğer bir deyişle, uygulamalar diğer uygulamaların [FLAG_SECURE](#) ayarlarını atlamak için geçici çözümler üretmemeli veya bunu kolaylaştırmamalıdır.

[Erişilebilirlik aracı](#) kategorisine giren uygulamalar, FLAG_SECURE işaretiyle korunan içerikleri kullanıcı cihazı dışından erişim için aktarmadığı, kaydetmediği veya ön belleğe almadığı sürece bu şarttan muaftır.

Cihaz üzerinde Android kapsayıcıları çalıştıran uygulamalar

Cihaz üzerinde Android kapsayıcı uygulamaları, Android OS'i tamamen ya da kısmen simüle eden ortamlar sağlar. Bu ortamlardaki deneyim [Android güvenlik özelliklerinin](#) tamamını yansıtmayabilir. Bu nedenle geliştiriciler, cihaz üzerinde Android kapsayıcılarının, simüle edilen Android ortamlarında çalışmaması gerektiğini belirtmek için güvenli ortam manifest işareti eklemeyi seçebilirler.

Güvenli ortam manifest işareti

[REQUIRE_SECURE_ENV](#) işareti, uygulamanın cihaz üzerinde Android kapsayıcı uygulamalarında çalıştırılmaması gerektiğini belirtmek için uygulama manifest dosyasına eklenebilir. Güvenlik ve gizlilik nedeniyle, cihaz üzerinde Android kapsayıcısı sağlayan uygulamaların bu işareti taşıyan hiçbir uygulamada çalıştırılmaması gerekir. Ayrıca bu uygulamalar:

- Cihaz üzerinde Android kapsayıcılarına yüklemeyi planladıkları uygulamaların manifest'lerini inceleyerek bu işaretin olup olmadığını kontrol etmelidir.
- Bu işareti beyan eden uygulamaları, cihaz üzerinde Android kapsayıcılarına yüklememelidir.
- Cihazda API'leri çağırarak veya engelleyerek proxy gibi çalışmamalı, bunların kapsayıcıda yüklü olduğu izlenimi yaratmamalıdır.
- İşareti atlamak için geçici çözümler (ör. mevcut uygulamanın REQUIRE_SECURE_ENV işaretini atlamak için eski sürümünü yüklemek) üretmemeli veya bunu kolaylaştırmamalıdır.

Bu politikayla ilgili daha fazla bilgiyi [Yardım Merkezimizde](#) bulabilirsiniz.

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/videolar 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.

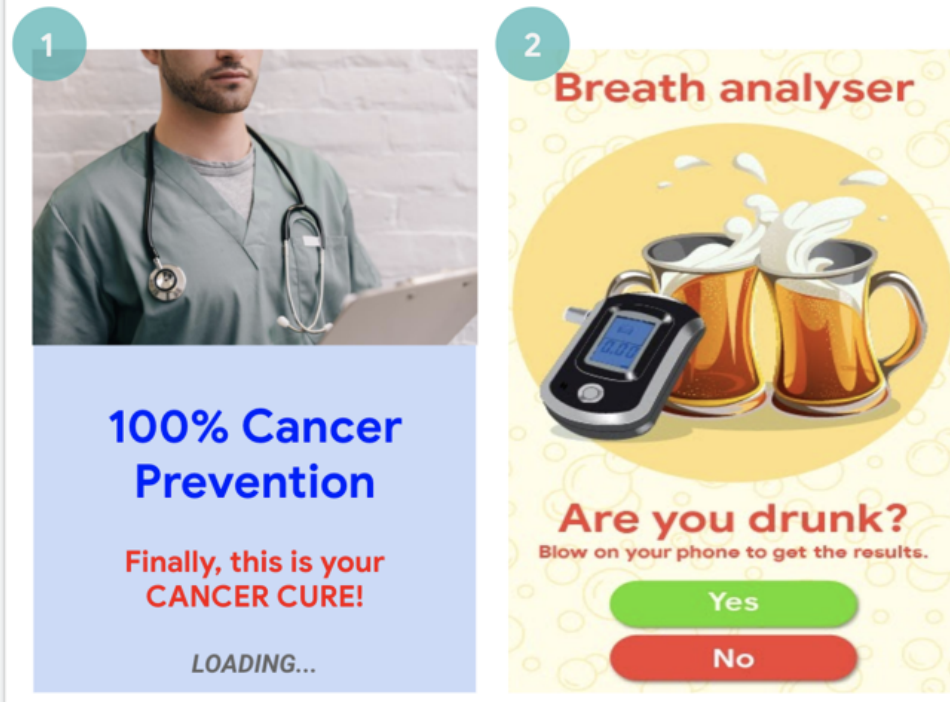
Yanıltıcı İddialar

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 kaldırılacağını açıkladığı bir yol gösterici metin içeren 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
- Oy verme süreçlerini etkileyebilecek şekilde veya seçim sonuçlarıyla ilgili yanıltıcı ya da yanlış olduğu kanıtlanabilir içerik

- Gerçekte olmadığı halde bir devlet kuruluşuyla bağlantılı olduğunu iddia eden veya gerekli yetkiye sahip olmadığı halde resmî hizmetler 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, kısıyollar, simgeler, widget'lar ve uygulamaların ana ekranda gösterilme şekli bulunur.

Ayrıca, şunlara da izin verilmez:

- Cihaz ayarlarını veya özelliklerini 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 özendiren uygulamalar.

Dürüst Olmayan Davranışlara İmkan Verme

Kimlik kartları, vatandaşlık numaraları, pasaportlar, diplomalar, kredi kartları, banka hesapları 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 uyardan (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, indiriminin içerik yayınlama ağı (CDN) ile desteklendiği uygulamalar.

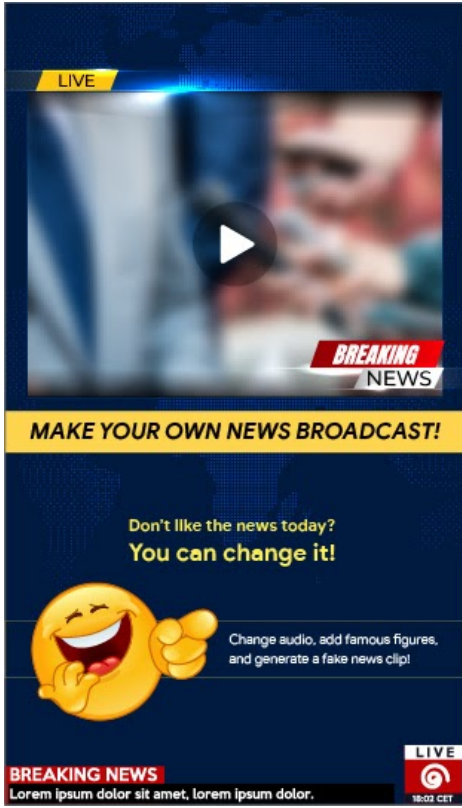
İçeriği Çarpıtılmış Medya

Görüntü, ses, video 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.

Davranış Şeffaflığı

Uygulamanızın işlevi, kullanıcılar açısından mümkün olduğunca açık olmalıdır. Uygulamanızda gizli, etkin olmayan veya belirtilmemiş özelliklere yer vermeyin. Uygulama incelemesinden kaçınma yöntemlerine izin verilmez. Kullanıcı güvenliğini, sistem bütünlüğünü ve politikalara uygunluğu sağlamak için uygulamalardan ek bilgiler istenebilir.

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 işbirliği yapmak.

Google Play'in Hedef API Düzeyi Politikası

Google Play, kullanıcılara güvenli bir deneyim sunmak için **tüm uygulamalarda** aşağıdaki hedef API düzeylerini zorunlu tutmaktadır:

Yeni uygulamaların ve uygulama güncellemelerinin, son Android ana sürümünün en fazla bir yıl öncesine ait olan bir Android API düzeyini hedeflemesi GEREKMEKTEDİR. Bu şartı karşılamayan yeni uygulamaların ve uygulama güncellemelerinin, Play Console'da uygulama göndermesi engellenecektir.

Güncellenmemiş ve yayınlanan son Android ana sürümünden en fazla iki yıl öncesine ait olan bir API düzeyini hedeflemeyen uygulamalar, cihazları Android OS'in daha yeni sürümlerini çalıştıran yeni kullanıcılara sunulmayacaktır. Uygulamayı daha önce Google Play Store'dan yüklemiş olan kullanıcılar, uygulamanın desteklediği tüm Android OS sürümlerinde uygulamayı keşfetmeye, yeniden yüklemeye ve kullanmaya devam edebilecektir.

Hedef API düzeyi şartının nasıl karşılanacağıyla ilgili teknik tavsiye için lütfen [taşıma rehberini](#) inceleyin.

Tüm zaman çizelgeleri ve istisnalar için lütfen bu [Yardım Merkezi makalesine](#) bakın.

SDK Şartları

Uygulama geliştiriciler, uygulamalarına temel işlevleri ve hizmetleri entegre etmek için genellikle üçüncü taraf kodlarını (ör. SDK) kullanırlar. Uygulamanıza SDK eklerken kullanıcılarınızın güvenliğini sağlamanız ve uygulamanızı güvenlik açıklarından korumanız gerekir. Bu bölümde, mevcut gizlilik ve güvenlik şartlarımızdan SDK'larla ilgili olanlar ele alınmaktadır. Ayrıca, bu şartların, geliştiricilerin SDK'ları uygulamalarına güvenli bir şekilde entegre etmesine nasıl yardımcı olduğu açıklanmaktadır.

Uygulamanıza eklediğiniz SDK'nın üçüncü taraf kodu ve davranışları, uygulamanızın Google Play Geliştirici Program Politikaları'nı ihlal etmesine yol açmamalıdır. Bunu sağlamak sizin sorumluluğunuzdadır. Uygulamanızdaki SDK'ların kullanıcı verilerini nasıl işlediğine dikkat etmek, hangi izinleri kullandıklarını ve hangi verileri topladıklarını nedenleriyle birlikte bilmek önemlidir. SDK'lar, kullanıcı verilerini, uygulamanızın politikayla uyumlu veri kullanımına uygun şekilde toplamalı ve işlemelidir.

SDK'yı kullanırken politika şartlarını ihlal etmemek için aşağıdaki politikaları eksiksiz bir şekilde okuyup anlayın ve SDK'larla ilgili aşağıdaki şartlara dikkat edin:

Kullanıcı Verileri Politikası

Kullanıcı verilerini (ör. cihaz bilgileri de dahil bir kullanıcıdan alınan veya kullanıcı hakkında toplanan bilgiler) nasıl kullandığınız konusunda şeffaf olmalısınız. Bu gereklilik, uygulamanızdan kullanıcı verilerine erişim, verileri toplama, kullanma, işleme ve paylaşma süreçlerinin açıklanması ve verilerin yalnızca politikaya uygun olduğu belirtilen amaçlarla kullanılması anlamına gelir.

Uygulamanıza üçüncü taraf kodu (ör. bir SDK) eklerseniz uygulamanızda kullanılan üçüncü taraf kodunun ve bu üçüncü tarafın uygulamanızdaki kullanıcı verileriyle ilgili yaklaşımının, kullanım ve açıklama şartları da dahil olmak üzere Google Play Geliştirici Program Politikaları'na uygun olmasını sağlamanız gerekir. Örneğin, SDK sağlayıcılarınızın uygulamanızdaki kişisel ve hassas kullanıcı verilerini satmamasını sağlamalısınız. Bu şart hem sunucuya gönderildikten sonra aktarılan hem de uygulamanıza üçüncü taraf kodu yerleştirilerek aktarılan kullanıcı verileri için geçerlidir.

Kişisel ve Hassas Kullanıcı Verileri

- Uygulama aracılığıyla edinilen kişisel ve hassas kullanıcı verileriyle ilgili erişim, toplama, kullanım ve paylaşım sürecini, uygulama ve hizmet işleviyle ve makul ölçüde kullanıcıdan beklenebilecek politikaya uygun amaçlarla sınırlandırmalısınız:
 - Kişisel ve hassas kullanıcı verilerinin kullanım kapsamını reklam yayınlamak için genişleten uygulamalar, Google Play'in Reklam Politikası'na uygun olmalıdır.
- Modern kriptografi kullanarak iletme (örneğin, HTTPS üzerinden) de dahil olmak üzere tüm kişisel ve hassas kullanıcı verilerini güvenli bir şekilde işlemelisiniz.
- Mümkün olduğunda her zaman, Android izinleriyle korunan verilere erişmeden önce çalışma zamanı izni istemelisiniz.

Kişisel ve Hassas Kullanıcı Verilerinin Satışı

Kişisel ve hassas kullanıcı verilerini satmamalısınız.

- "Satış", kişisel ve hassas kullanıcı verilerinin para kazanma amacıyla üçüncü taraflara aktarılmasını veya veri alışverişini ifade eder.
- Kullanıcılar tarafından başlatılan kişisel ve hassas kullanıcı verisi aktarımı (ör. kullanıcı, uygulamanın bir özelliğini kullanarak üçüncü bir tarafa dosya aktardığında veya özel amaca yönelik araştırma uygulaması kullandığında) satış olarak değerlendirilmez.

Belirgin Açıklama ve Rıza Şartları

Uygulamanızın, kişisel ve hassas kullanıcı verilerine erişme, verileri toplama, kullanma veya paylaşma süreçleri, söz konusu ürün ya da özelliğin kullanıcılarından makul ölçüde beklenebilecek amaçların dışındaysa [Kullanıcı Verileri Politikası](#)'nın belirgin açıklama ve rıza şartlarına uymanız gerekir.

Uygulamanıza varsayılan olarak kişisel ve hassas kullanıcı verilerini toplamak üzere tasarlanmış bir üçüncü taraf kodu (ör. bir SDK) entegre edilmişse Google Play'den talep aldıktan sonra iki hafta içinde (ya da Google Play'in talebinde belirtilen süre zarfında) uygulamanızın bu politikanın belirgin açıklama ve rıza şartını (üçüncü taraf kodu aracılığıyla veri paylaşımı, erişimi, toplanması veya kullanımı açısından dahil) yerine getirdiğini gösteren yeterli kanıt sunmanız gerekir.

Üçüncü taraf kodunu (ör. SDK), [Kullanıcı Verileri Politikası](#)'nı ihlal etmeyecek şekilde kullanmanız gerektiğini unutmayın.

Belirgin açıklama ve rıza şartı hakkında daha fazla bilgi için bu [Yardım Merkezi makalesini](#) inceleyebilirsiniz.

SDK kaynaklı ihlallere örnekler

- Kişisel ve hassas kullanıcı verilerini toplayan bir SDK içeren ancak bu verileri bu Kullanıcı Verileri Politikası'na, erişim, veri işlemenin yanı sıra (izin verilmeyen satış dahil) belirgin açıklama ve rıza şartlarına tabi olarak değerlendirmeyen uygulamalar
- Bu politikanın kullanıcı rızası ve belirgin açıklama şartlarını ihlal edecek şekilde varsayılan olarak kişisel ve hassas kullanıcı verilerini toplayan bir SDK içeren uygulamalar
- Kişisel ve hassas kullanıcı verilerini yalnızca uygulamaya sahtekarlıkla ve kötüye kullanımla mücadele işlevi sağlamak amacıyla topladığını iddia eden ancak topladığı verileri reklam veya analiz için üçüncü taraflarla da paylaşan bir SDK içeren uygulamalar
- Kullanıcıların cihazlarında yüklü paket bilgisini, belirgin açıklama yönergelerine ve/veya [gizlilik politikası yönergelerine](#) uygun olmayan şekilde ileten bir SDK içeren uygulamalar
 - [İstenmeyen Mobil Yazılım Politikası](#)'na da göz atın.

Kişisel ve Hassas Verilere Erişimle İlgili Ek Şartlar

Aşağıdaki tabloda, belirli etkinliklerle ilgili şartlar açıklanmaktadır.

Etkinlik	Şartlar
Uygulamanız kalıcı cihaz tanımlayıcıları topluyor veya bunlara bağlantı veriyor (ör. IMEI, IMSI, SIM Seri Numarası vb.)	Kalıcı cihaz tanımlayıcıları, aşağıdaki amaçlar dışında diğer kişisel ve hassas kullanıcı verilerine veya sıfırlanabilir cihaz tanımlayıcılarına bağlanamaz: • SIM kimliğine (ör. operatörün hesabına bağlı kablosuz arama) bağlı telefon işlevleri ve • Cihaz sahibi modunu kullanan kurumsal cihaz yönetim uygulamaları. Bu kullanımlar, Kullanıcı Verileri Politikası 'nda belirtildiği gibi kullanıcılara belirgin bir şekilde açıklanmalıdır. Alternatif benzersiz tanımlayıcılar için lütfen bu kaynağa bakın . Android reklam kimliği ile ilgili ek yönergeler hakkında bilgi edinmek için lütfen Reklam Politikası 'nı okuyun.
Uygulamanız çocukları hedefliyor	Uygulamanıza eklediğiniz SDK'nın çocuklara yönelik hizmetlerde kullanım için içerik üretici onayı almış olması şarttır. Politikayı ve şartlarını Aileler İçin İçerik Üretici Onaylı Reklam SDK'sı Programı başlıklı makalede eksiksiz bir şekilde bulabilirsiniz.

SDK kaynaklı ihlallere örnekler

- Android kimliği ile konumu bağlayan bir SDK kullanan uygulamalar
- AAID'yi reklam veya analiz için kalıcı cihaz tanımlayıcılarına bağlayan bir SDK içeren uygulamalar
- AAID'yi analiz için e-posta adresine bağlayan bir SDK içeren uygulamalar

Veri güvenliği bölümü

Tüm geliştiriciler, her uygulama için kullanıcı verilerinin nasıl toplandığını, kullanıldığını ve paylaşıldığını açıklayan Veri Güvenliği bölümü hazırlamalıdır. Bu açıklamadaki bilgilerin kolay anlaşılabilir ve doğru olması gerekir. Buna, uygulamalarda kullanılan tüm üçüncü taraf kitaplıklar veya SDK'lar üzerinden toplanan ve işlenen veriler dahildir. Etiketin doğruluğu ve bu bilgilerin güncel tutulması geliştiricinin sorumluluğundadır. Veri Güvenliği bölümü, uygulamanın gizlilik politikasında yapılan açıklamaların ilgili kısımlarıyla tutarlı olmalıdır.

Veri Güvenliği bölümünü doldurmayla ilgili daha fazla bilgiyi bu [Yardım Merkezi makalesinde](#) bulabilirsiniz.

[Kullanıcı Verileri Politikası](#)'nın tamamını inceleyin.

Hassas Bilgilere Erişen İzinler ve API'ler Politikası

İzin talepleri ve hassas bilgilere erişimi olan API'ler, kullanıcılar açısından anlamlı olmalıdır. Yalnızca Google Play girişinizde tanıtılan mevcut özelliklerin veya hizmetlerin uygulamanızda kullanılabilmesi için gereken izinleri ve hassas bilgilere erişimi olan API'leri isteyebilirsiniz. Açıklanmayan, henüz uygulanmamış veya izin verilmeyen özellikler ya da amaçlar için kullanıcı veya cihaz verilerine erişim sağlayan izinleri ya da hassas bilgilere erişimi olan API'leri kullanamazsınız. İzinler veya hassas bilgilere erişimi olan API'ler üzerinden erişilen kişisel veya hassas veriler hiçbir zaman satılamaz ya da satışı kolaylaştıracak bir amaç doğrultusunda paylaşılamaz.

[Hassas Bilgilere Erişen İzinler ve API'ler Politikası](#)'nın tamamını inceleyin.

SDK kaynaklı ihlallere örnekler

- İzin verilmeyen veya açıklanmamış bir amaç için arka planda konum bilgisi isteyen bir SDK içeren uygulamalar
- Kullanıcının rızası olmadan read_phone_state Android izninden elde edilmiş IMEI bilgisini ileten bir SDK içeren uygulamalar

Kötü Amaçlı Yazılım Politikası

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.

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.

Bu politikanın şartları ayrıca uygulamanıza dahil ettiğiniz tüm üçüncü taraf kodlar (örneğin, SDK) için de geçerlidir.

[Kötü Amaçlı Yazılım Politikası](#)'nın tamamını inceleyin.

SDK kaynaklı ihlallere örnekler

- Kötü amaçlı yazılım dağıtan sağlayıcıların SDK kitaplıklarını içeren uygulamalar
- Android izin modelini ihlal eden veya diğer uygulamalardan kimlik bilgilerini (ör. OAuth jetonları) çalan uygulamalar
- Yüklemelerinin kaldırılmasını veya durdurulmalarını önleyen özellikleri kötüye kullanan uygulamalar
- SELinux'u devre dışı bırakan uygulamalar

- Açıklanmamış bir amaç için cihaz verilerine erişip üst düzey ayrıcalıklar elde ederek Android izin modelini ihlal eden bir SDK içeren uygulamalar
- İçerdiği kodla kullanıcıları kandırarak cep telefonu faturaları aracılığıyla içeriklere abone olmalarını veya içerik satın almalarını sağlayan bir SDK içeren uygulamalar

Uygulamalarda SDK Kullanımı

Uygulamanıza eklediğiniz SDK'nın üçüncü taraf kodu ve davranışları, uygulamanızın Google Play Geliştirici Program Politikaları'nı ihlal etmesine yol açmamalıdır. Bunu sağlamak sizin sorumluluğunuzdadır. Uygulamanızdaki SDK'ların kullanıcı verilerini nasıl işlediğine dikkat etmek, hangi izinleri kullandıklarını ve hangi verileri topladıklarını nedenleriyle birlikte bilmek önemlidir.

SDK Şartları

Uygulama geliştiriciler, uygulamalarına temel işlevleri ve hizmetleri entegre etmek için genellikle üçüncü taraf kodlarını (ör. SDK) kullanırlar. Uygulamanıza SDK eklerken kullanıcılarınızın güvenliğini sağlamanız ve uygulamanızı güvenlik açıklarından korumanız gerekir. Bu bölümde, mevcut gizlilik ve güvenlik şartlarımızdan SDK'larla ilgili olanlar ele alınmaktadır. Ayrıca, bu şartların, geliştiricilerin SDK'ları uygulamalarına güvenli bir şekilde entegre etmesine nasıl yardımcı olduğu açıklanmaktadır.

Uygulamanıza eklediğiniz SDK'nın üçüncü taraf kodu ve davranışları, uygulamanızın Google Play Geliştirici Program Politikaları'nı ihlal etmesine yol açmamalıdır. Bunu sağlamak sizin sorumluluğunuzdadır. Uygulamanızdaki SDK'ların kullanıcı verilerini nasıl işlediğine dikkat etmek, hangi izinleri kullandıklarını ve hangi verileri topladıklarını nedenleriyle birlikte bilmek önemlidir. SDK'lar, kullanıcı verilerini, uygulamanızın politikayla uyumlu veri kullanımına uygun şekilde toplamalı ve işlemelidir.

SDK'yı kullanırken politika şartlarını ihlal etmemek için aşağıdaki politikaları eksiksiz bir şekilde okuyup anlayın ve SDK'larla ilgili aşağıdaki şartlara dikkat edin:

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

Casus yazılım

Casus yazılım, politikayla uyumlu işlevlerle ilgili olmayan kullanıcı ya da cihaz verilerini toplayan, çalan veya paylaşan kötü amaçlı bir uygulama, kod ya da davranıştır.

Kullanıcıyı gizlice izleme kapsamında değerlendirilebilecek veya yeterli bildirim ya da izin olmaksızın verileri çalan kötü amaçlı kod veya davranışlar da casus yazılım olarak kabul edilir.

[Casus Yazılım Politikası](#)'nın tamamını inceleyin.

Örneğin, SDK kaynaklı casus yazılım ihlallerine aşağıdakiler örnek verilebilir ancak örnekler bunlarla sınırlı değildir:

- Politikaya uygun uygulama işlevselliğiyle ilgili olmamasına rağmen ses veya arama kayıtlarından veri aktaran SDK'ları kullanan uygulamalar
- Kullanıcının beklemediği bir şekilde ve/veya yeterli kullanıcı bildirimi ya da izni olmaksızın cihazdaki verileri aktaran kötü amaçlı üçüncü taraf kodu (örneğin, SDK) içeren uygulamalar

İstenmeyen Mobil Yazılım Politikası

Şeffaf davranış ve net açıklamalar

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

Örnek ihlaller:

- Reklam sahtekarlığı
- Sosyal Mühendislik

Kullanıcı verilerini koruma

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 Politikaları'na uyulmalı ve verileri korumak için tüm önlemler alınmalıdır.

Örnek ihaller:

- Veri Toplama (Casus yazılım)
- Kısıtlanmış izinlerin kötüye kullanımı

[İstenmeyen Mobil Yazılım Politikası](#)'nın tamamını inceleyin.

Cihazları ve Ağı Kötüye Kullanma Politikası

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.

Çalıştırma zamanında yüklenen (ör. uygulamaya paket olarak eklenmemiş), yorumlanmış dillere (JavaScript, Python, Lua vb.) sahip uygulamalar veya üçüncü taraf kodları (ör. SDK'lar), Google Play politikalarının olası ihlallerine izin vermemelidir.

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.

[Cihazları ve Ağı Kötüye Kullanma Politikası](#)'nın tamamını inceleyin.

SDK kaynaklı ihallere örnekler

- Üçüncü taraflara proxy hizmetlerini kolaylaştıran uygulamalar bunu yalnızca uygulamanın birincil, kullanıcıya yönelik temel amacı olduğu takdirde yapabilir.
- Google Play dışında bir kaynaktan dex dosyası veya yerel kod gibi yürütülebilir kodlar indiren bir SDK içeren uygulamalar
- Güvenilir olmayan web içeriklerini (örneğin, http:// URL) veya güvenilir olmayan kaynaklardan alınan doğrulanmamış URL'leri (örneğin, güvenilir olmayan niyetlerle elde edilen URL'ler) yükleyen JavaScript arayüzü eklenmiş web görünümü içeren bir SDK barındıran uygulamalar
- Kendi APK'sını güncellemek için kullanılan kodu içeren bir SDK barındıran uygulamalar
- Güvenli olmayan bir bağlantı üzerinden dosya indirerek kullanıcıları güvenlik açığına maruz bırakan bir SDK içeren uygulamalar
- Google Play dışındaki bilinmeyen kaynaklardan uygulama indirmeye veya yüklemeye yarayan kodlar içeren bir SDK barındıran uygulamalar
- Uygun bir kullanım alanı olmadan ön plan hizmetlerinin kullanıldığı bir SDK barındıran uygulamalar
- Politikaya uygun bir nedenden dolayı ön plan hizmetlerini kullanan, ancak uygulamanızın manifest dosyasında beyan edilmemiş bir SDK barındıran uygulamalar

Yanıltıcı Davranış Politikası

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/videolar 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.

[Yanıtıcı Davranış Politikası](#)'nın tamamını görün.

Davranış Şeffaflığı

Uygulamanızın işlevi, kullanıcılar açısından mümkün olduğunca açık olmalıdır. Uygulamanızda gizli, etkin olmayan veya belirtilmemiş özelliklere yer vermeyin. Uygulama incelemesinden kaçınma yöntemlerine izin verilmez. Kullanıcı gizliliğini, sistem bütünlüğünü ve politikalara uygunluğu sağlamak için uygulamalardan ek bilgiler istenebilir.

SDK'dan kaynaklanan ihlal örneği

- Uygulamanız, uygulama incelemelerinden kaçınmayı sağlayacak tekniklerin kullanıldığı bir SDK içeriyor.

SDK kaynaklı ihlallerle yaygın olarak ilişkilendirilen Google Play Geliştirici Politikaları

Uygulamanızın kullandığı tüm üçüncü taraf kodlarının Google Play'in Geliştirici Program Politikaları'na uymasını sağlamak için lütfen aşağıdaki politikaları eksiksiz bir şekilde inceleyin:

- [Kullanıcı Verileri Politikası](#)
- [Hassas Bilgilere Erişen İzinler ve API'ler](#)
- [Cihazları ve Ağ Kötüye Kullanma Politikası](#)
- [Kötü Amaçlı Yazılım](#)
- [Mobil İstenmeyen Yazılım](#)
- [Aileler İçin İçerik Üretici Onaylı Reklam SDK'sı Programı](#)
- [Reklam Politikası](#)
- [Yanıtıcı Davranış](#)
- [Google Play Geliştirici Program Politikaları](#)

Daha çok yukarıda belirtilen politikalar referans gösterilse de uygulamanızın, geçersiz SDK kodu nedeniyle başka politikaları da ihlal edebileceğini unutmayın. Uygulama geliştirici olarak SDK'larınızın uygulama verilerinizi politikalara uygun şekilde işlemesini sağlamak sizin sorumluluğunuzdadır. Bu nedenle, tüm politikaları eksiksiz bir şekilde incelemeyi ve politika güncellemelerini takip etmeyi unutmayın.

Daha fazla bilgi edinmek için lütfen [Yardım Merkezimizi](#) ziyaret edin.

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.

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.

Bu politikanın şartları ayrıca uygulamanıza dahil ettiğiniz tüm üçüncü taraf kodlar (örneğin, SDK) için de geçerlidir.

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 saldırganın, 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 ağları 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 yararlandığını 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 gerçekleştirilebileceğini 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.

Telefonla Arama Sahtekarlığı

Kullanıcının izni olmadan premium numaraları arayarak kullanıcıdan ödeme alan kod.

Ücret Sahtekarlığı

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

Ücret 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

İzleme amacıyla cihazlardan kişisel veya hassas kullanıcı verilerini toplayıp üçüncü taraflara (şirket veya başka bir şahıs) aktaran kod.

Uygulamalar, [Kullanıcı Verileri Politikası](#) uyarınca öne çıkan açıklama sağlamalı ve kullanıcılardan izin almalıdır.

İzleme Uygulamalarıyla İlgili Yönergeler

Kabul edilebilir yegane izleme uygulamaları; aşağıda açıklanan şartlara bütünüyle uymaları koşuluyla, özel olarak başka bir kişinin izlenmesi (ör. ebeveynlerin çocuklarını izlemeleri veya şirket yönetiminin çalışanları izlemesi) amacıyla tasarlanmış ve bu şekilde pazarlanan uygulamalardır. Bu uygulamalar, kalıcı bildirim görüntülenmesinden bağımsız olarak haberi ve izni olsa dahi herhangi başka bir kişiyi (örneğin, eşi) takip etmek için kullanılamaz. Bu uygulamaların kendilerini izleme uygulamaları olarak tanımlayabilmesi için manifest dosyalarında IsMonitoringTool meta veri işaretini kullanması gerekir.

İzleme uygulamalarının uyması gereken şartlar şunlardır:

- 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, kullanıcıya uygulama çalıştığı sürece kalıcı bir bildirim ve uygulamayı açıkça tanımlayan benzersiz bir simge sunmalıdır.
- Uygulamalar, izleme veya takip işlevini Google Play Store açıklamasında belirtmelidir.
- 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).
- Uygulamalar tüm geçerli yasalara uymalıdır. Uygulamanızın, hedeflendiği yerel bölgede yasal olup olmadığını belirleme konusunda tüm sorumluluk size aittir.

Daha fazla bilgi için lütfen [IsMonitoringTool işaretinin kullanımı](#) başlıklı Yardım Merkezi makalesine bakın.

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 bildirirse 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

Casus yazılım, politikayla uyumlu işlevlerle ilgili olmayan kullanıcı ya da cihaz verilerini toplayan, çalan veya paylaşan kötü amaçlı bir uygulama, kod ya da davranıştır.

Kullanıcıyı gizlice izleme kapsamında değerlendirilebilecek veya yeterli bildirim ya da izin olmaksızın verileri çalan kötü amaçlı kod veya davranışlar da casus yazılım olarak kabul edilir.

Örneğin, bunlarla sınırlı olmamakla birlikte casus yazılım ihlallerine şu örnekler verilebilir:

- Sesleri veya telefona gelen aramaları kaydetme
- Uygulama verilerini çalma
- Kullanıcının beklemediği bir şekilde ve/veya yeterli kullanıcı bildirimi ya da izni olmaksızın cihazdaki verileri aktaran kötü amaçlı üçüncü taraf kodu (örneğin, SDK) içeren uygulama

Tüm uygulamalar aynı zamanda [İstenmeyen Mobil Yazılım](#), [Kullanıcı Verileri](#), [Hassas Bilgilere Erişen İzinler ve API'ler](#), [SDK Şartları](#) gibi kullanıcı ve cihaz verileri politikaları dahil olmak üzere tüm Google Play Geliştirici Program Politikaları'na da uymalıdır.

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.

Maskware

Kullanıcıya farklı veya sahte uygulama işlevi sunmak için çeşitli kaçınma tekniklerinden yararlanan uygulamalardır. Bu uygulamalar, uygulama mağazalarına zararsız görünmek için kendilerini meşru uygulamalar veya oyunlar olarak maskeler ve kötü amaçlı içeriğin fark edilmemesi için kod karartma, dinamik kod yükleme veya gizleme gibi teknikler kullanır.

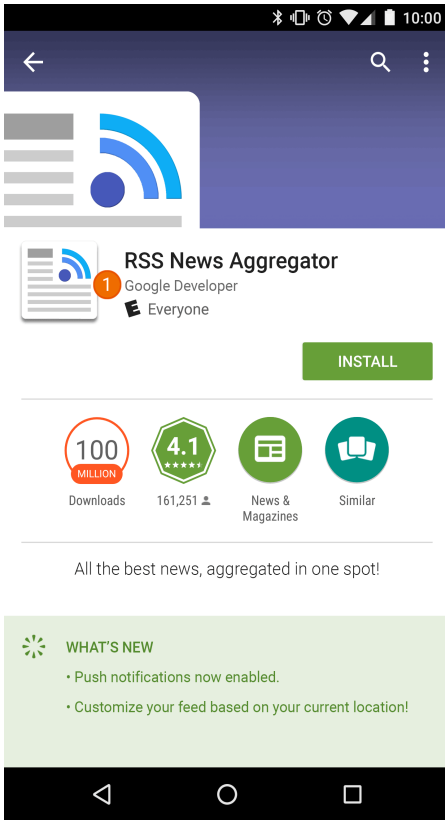
Maskeli yazılımlar, başta truva atı olmak üzere diğer PHA kategorilerine benzer. Aralarındaki temel fark, kötü amaçlı etkinliği gizlemek için farklı tekniklerin kullanılmasıdır.

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/tüzel kişi/kuruluş 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.

- Öyle olmadığı halde başka bir şirket/geliştirici/tüzel kişi/kuruluş ile ilişkisi olduğunu ima eden simgeler ve başlıklar kullanan uygulamalar

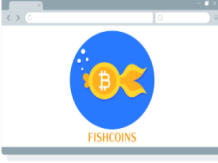
✓		
✗	① 	② 

①Uygulama, yanıltıcı şekilde ulusal bir amblem kullanarak kullanıcıları devletle bağlantılı olduğuna inandırıyor.

②Uygulama, ticari bir işletmenin logosunu kullanarak öyle olmadığı halde o işletmenin resmi uygulaması gibi davranıyor.

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

✓				
✗				

✓		
✗	① 	② 

①Uygulama, simgesinde popüler bir kripto para biriminin web sitesinin logosunu kullanarak o sitenin resmi uygulaması gibi davranıyor.

②Uygulama, simgesinde ünlü bir TV programının karakter ve başlığını kullanarak öyle olmadığı halde TV programıyla bağlantılıymış izlenimi yaratıyor.

- 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.
- [Android Markalama Kuralları](#) 'nı ihlal eden uygulamalar

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
- Sosyal Mühendislik

Kullanıcı verilerini ve gizliliğini koruma

Kişisel ve hassas kullanıcı verilerine erişme, bu verileri kullanma, toplama ve paylaşma konularında net ve şeffaf olun. Kullanıcı verilerini kullanırken, geçerli durumlarda ilgili tüm kullanıcı verileri politikalarına uyulmalı ve verileri korumak için tüm önlemler alınmalıdır.

Tüm uygulamalar; [Kullanıcı Verileri](#), [Hassas Bilgilere Erişen İzinler ve API'ler](#), [Casus Yazılımlar](#) ve [SDK Şartları](#) gibi kullanıcı ve cihaz verileri politikaları da dahil olmak üzere tüm Google Play Geliştirici Program Politikaları'na uymak zorundadır.

- Kullanıcılardan Google Play Protect gibi cihaz güvenliği korumalarını devre dışı bırakmalarını istemeyin veya bunu yapmaları için onları kandırmaya çalışmayın. Örneğin, kullanıcılara Google Play Protect'i devre dışı bırakmaları karşılığında ilave uygulama özellikleri veya ödüller sunamazsınız.

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

Zararlı İndirme Araçları

Kendi başına istenmeyen yazılım olmayan ancak başka mobil istenmeyen yazılımlar (MUWS) indiren kod.

Aşağıdaki durumlarda kodun zararlı bir indirme aracı olduğu söylenebilir:

- Kodun MUWS'leri yaymak için oluşturulduğuna veya MUWS'leri 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 MUWS'ler ise (25 gözlenen MUWS indirme işlemi).

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

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

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:

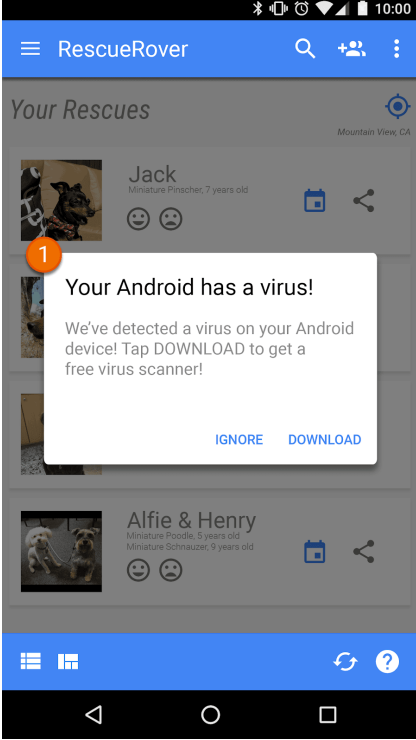
- Kullanıcı tarafından görülemeyen reklamlar oluşturan bir uygulama.
- Kullanıcının niyeti olmadan otomatik olarak reklamlara tıklama kazandıran veya hileli bir şekilde tıklama kredisi vermek için eşdeğer ağ trafiği oluşturan bir uygulama.
- Gönderenin ağından gelmeyen yüklemelerden para kazanmak için 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 uygulama ya da reklamlara izin vermeyiz. 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.

Sosyal Mühendislik

Kendisini başka bir uygulamaymış gibi gösterip kullanıcıları güvendikleri asıl uygulama için işlem yaptıkları yanılgısına düşürerek kandırmayı amaçlayan uygulamalara izin verilmez.

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 deneyiminin sağlanması için bu politikalara uyulmasını zorunlu tutuyoruz.

Ödemeler

1. Google Play'deki uygulama indirme işlemlerinden ücret alan geliştiriciler, bu işlemlerde ödeme yöntemi olarak Google Play'in faturalandırma sistemini kullanmalıdır.

2. Play'de dağıtılan bir uygulama; uygulama işlevselliği, dijital içerikler veya öğeler (hepsi birden "uygulama içi satın almalar" olarak adlandırılır) dahil olmak üzere uygulama içi özelliklere ya da hizmetlere erişim için ödeme gerektiriyor veya kabul ediyorsa, 3. 8. veya 9. bölümün geçerli olduğu durumlar dışında Google Play'in faturalandırma sistemini kullanmalıdır.

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)
- Abonelik hizmetleri (ör. fitness, oyun, arkadaşlık, eğitim, müzik, video, hizmet yükseltmeleri ve diğer içerik aboneliği hizmetleri)
- Uygulama işlevselliği veya içerik (ör. bir uygulamanın reklamsız sürümü veya ücretsiz sürümde bulunmayan yeni özellikler)
- Uygulama içinde satın alınan bulut yazılımı ve hizmetleri (ör. veri depolama hizmetleri, iş verimliliği yazılımları ve finansal yönetim yazılımları)

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

a. Ödeme esasen:

- 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;

b. Ödemeler, karşılıklı ödemeleri, internet üzerinden düzenlenen açık artırmaları ve vergiden muaf bağışları içeriyorsa;

c. Ödeme, [Gerçek Parayla Kumar Oynama, Oyunlar ve Yarışmalar](#) politikasının [Kumar Uygulamaları](#) bölümünde tanımlandığı şekilde internette kumar oynamayı kolaylaştıran içerik veya hizmetler için yapılıyorsa;

d. Ödeme, Google'ın [Ödeme Merkezi İçerik Politikaları](#) kapsamında kabul edilemez sayılan ürün kategorileriyle ilgiliyse.

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.

4. Uygulamalar, 3., 8. ve 9. bölümde açıklanan koşullar dışında kullanıcıları Google Play'in faturalandırma sisteminden başka 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 içeriklerle ilgili uygulama içi tanıtımlar
- Uygulama içi web görünümleri, düğmeler, bağlantılar, mesajlar, reklamlar veya diğer harekete geçirici mesajlar
- 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

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

6. 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.

7. 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.
8. 3. bölümde açıklanan koşullar geçerli değilse Play'de dağıtılan uygulamaların geliştiricileri, bu [ülkelerdeki/bölgelerdeki](#) kullanıcıların uygulama içi satın almalara erişebilmesi için ödeme gerektiriyor veya kabul ediyorsa kullanıcılara bu işlemler için Google Play'in faturalandırma sistemine ek olarak uygulama içinde bir alternatif faturalandırma sistemi sunabilirler. Bunun için geliştiricilerin, ilgili programlara ait faturalandırma beyan formunu başarıyla doldurup buradaki ek şartları ve [program koşullarını](#) kabul etmeleri gerekir.
9. Play'de dağıtılan uygulamaların geliştiricileri, Avrupa Ekonomik Alanı'ndaki (AEA) kullanıcıları dijital uygulama içi özellikler ve hizmetler ile ilgili fırsatları tanıtmak gibi işlemler için uygulama dışına yönlendirebilirler. AEA'daki kullanıcıları uygulama dışına yönlendiren geliştiricilerin programa ait [beyan formunu](#) doğru şekilde doldurup buradaki ek şartları ve [program koşullarını](#) kabul etmeleri gerekir.

Not: Bu politikayla ilgili zaman çizelgelerini ve sık sorulan soruları görüntülemek için lütfen [Yardım Merkezimizi](#) ziyaret edin.

Reklamlar

Kaliteli bir deneyim sunmaya devam etmek için reklamınızın içeriği, kitlesi, kullanıcı deneyimi ve davranışının yanı sıra güvenliği ve gizliliğini de dikkate alırız. Reklamları ve bunlarla ilişkili teklifleri uygulamanızın bir parçası olarak değerlendirdiğimiz için bu konuda da diğer tüm Google Play politikalarına uymanız gerekir. Google Play'de çocukları hedefleyen bir uygulamadan para kazanıyorsanız reklamlarla ilgili ek şartlarımız da mevcuttur.

[Aldatıcı tanıtımları](#) nasıl ele aldığımız da dahil olmak üzere uygulama tanıtımı ve mağaza girişi politikalarımız hakkında daha fazla bilgiyi [buradan](#) öğrenebilirsiniz.

Reklam İçeriği

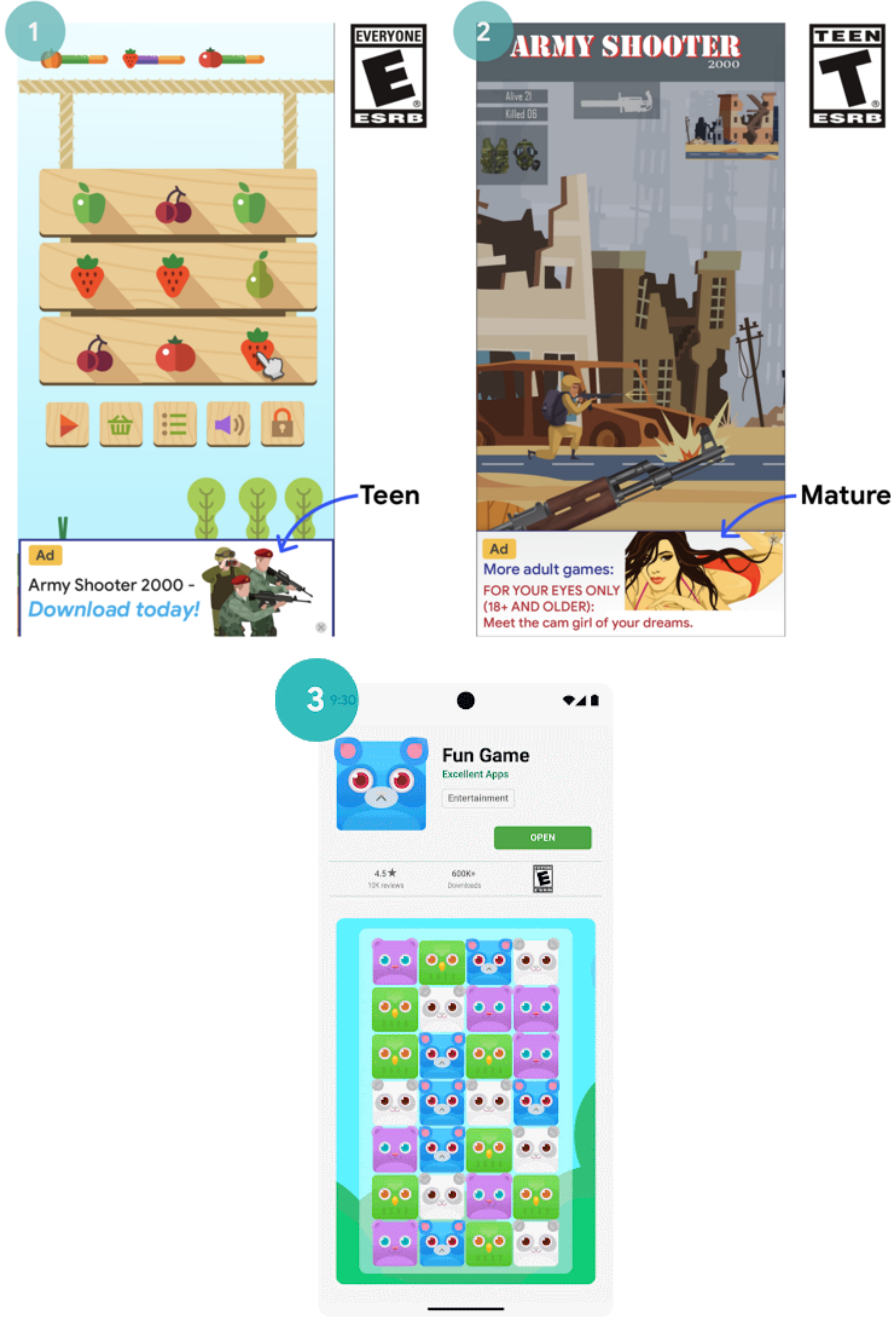
Reklamlar ve bunlarla ilişkili teklifler, uygulamanızın bir parçası olduğu için [Kısıtlanmış İçerik Politikalarımıza](#) uymalıdır. Uygulamanız bir [kumar](#) uygulamasıysa ek şartlar geçerlidir.

Uygunsuz Reklamlar

Uygulamanızda gösterilen reklamlar ve bunlarla ilişkili teklifler (ör. başka bir uygulamanın indirilmesini teşvik eden reklamlar), uygulamanızın [içerik derecelendirmesine](#) uygun olmalıdır (içerik kendi başına politikalarımıza uygun olsa bile).

Yaygın görülen ihlallere ilişkin bazı örnekleri aşağıda bulabilirsiniz:

- Uygulamanın içerik derecelendirmesine uygun olmayan reklamlar



- ① Bu reklam (Genç) bu uygulamanın içerik derecelendirmesi (Herkes) için uygunsuzdur.
- ② Bu reklam (Erişkin) bu uygulamanın içerik derecelendirmesi (Genç) için uygunsuzdur.
- ③ Reklamda sunulan teklif (Erişkin derecelendirmesine sahip bir uygulamanın indirilmesini teşvik ediyor.), reklamın gösterildiği oyun uygulamasının içerik derecelendirmesi (Herkes) için uygunsuzdur.

Aileler İçin Reklam Koşulları

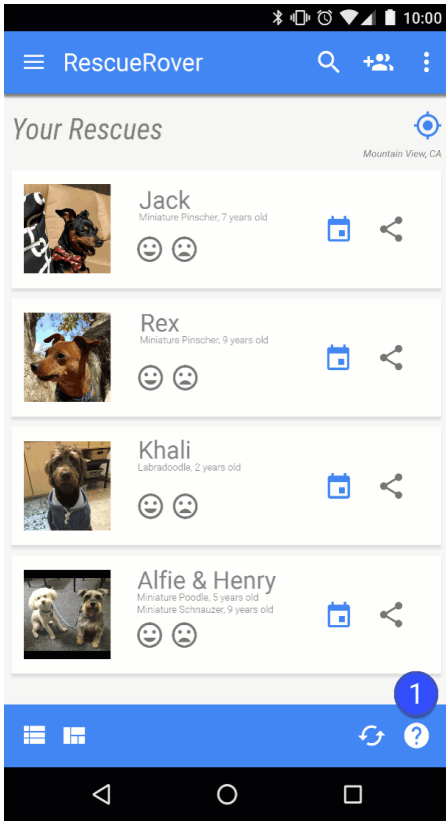
Google Play'de çocukları hedefleyen bir uygulamadan para kazanıyorsanız uygulamanızın [Aile Reklamları ve Para Kazanma Politikası Şartları](#)'na uyması önemlidir.

Yanıltıcı Reklamlar

Reklamlar hiçbir uygulama özelliğinin kullanıcı arayüzünü (ör. bir işletim sisteminin bildirimleri ya da uyarı öğeleri) taklit etmemeli veya bunların kimliğine bürünmemelidir. Her bir reklamı hangi uygulamanın sunduğu kolayca anlaşılmalıdır.

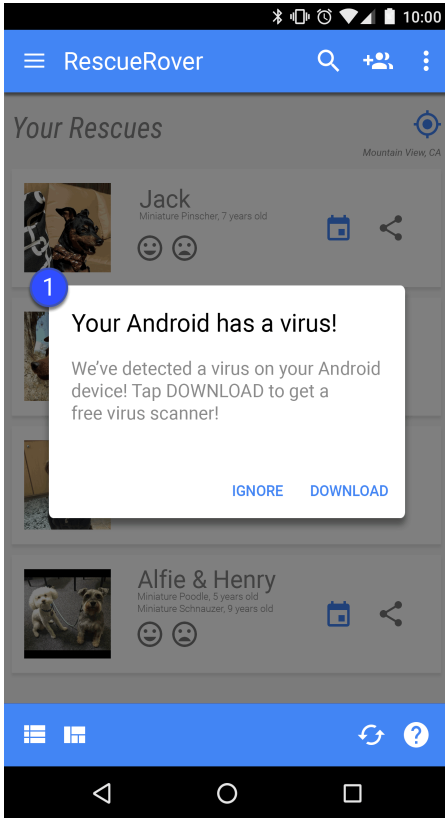
Yaygın görülen ihlallere ilişkin bazı örnekleri aşağıda bulabilirsiniz:

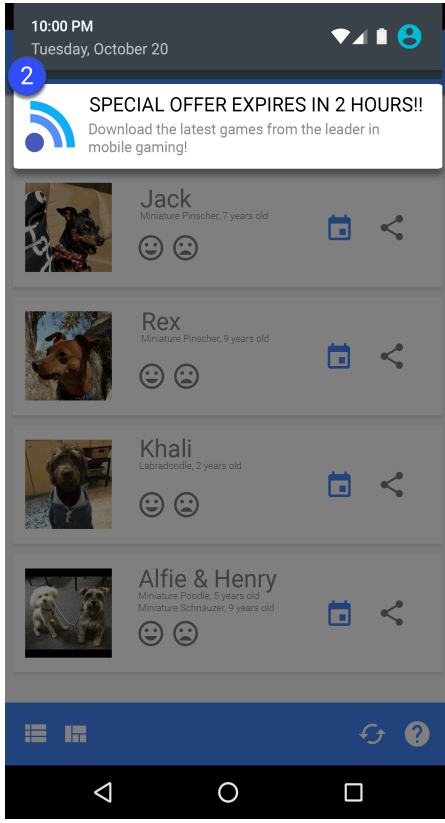
Bir uygulamanın kullanıcı arayüzünü taklit eden reklamlar:



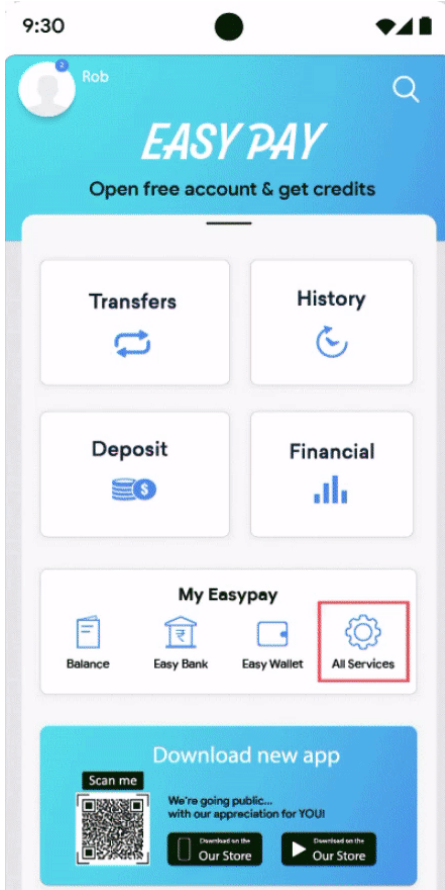
① Bu uygulamadaki soru işareti simgesi, kullanıcıyı harici bir açılış sayfasına yönlendiren bir reklamdır.

- Sistem bildirimlerini taklit eden reklamlar:





① ② Yukarıdaki örneklerde, çeşitli sistem bildirimlerini taklit eden reklamlar gösterilmektedir.



① Yukarıdaki örnekte, diğer özellikleri taklit eden ancak kullanıcıyı yalnızca bir veya daha fazla reklama yönlendiren bir özellik bölümü gösterilmektedir.

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. Reklamlar sadece bunları sunan uygulama içinde gösterilebilir. Ayrıca, başka uygulamalar, reklamlar veya sistem ya da cihaz düğmeleri ve bağlantı noktaları da dahil olmak üzere cihazın çalışmasını aksatmamalıdır. Bunlar arasında yer paylaşımları, tamamlayıcı öğelerin işlevleri ve widget haline getirilmiş reklam birimleri bulunur. Uygulamanız normal kullanımı aksatan reklamlar görüntülüyorsa bunların ceza olmadan kolayca kapatılabilmesi gerekir.

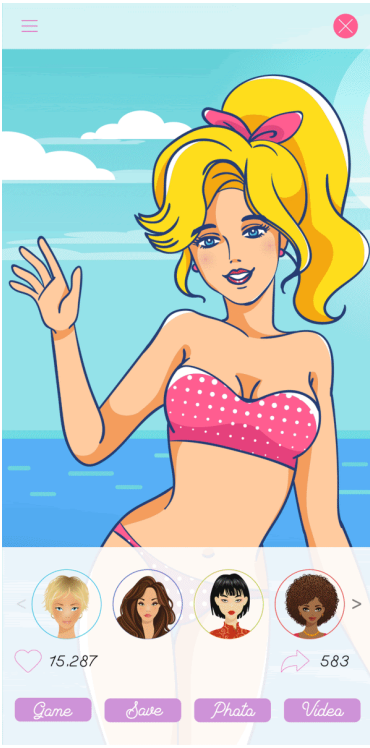
Yaygın görülen ihlallere ilişkin bazı örnekleri aşağıda bulabilirsiniz:

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

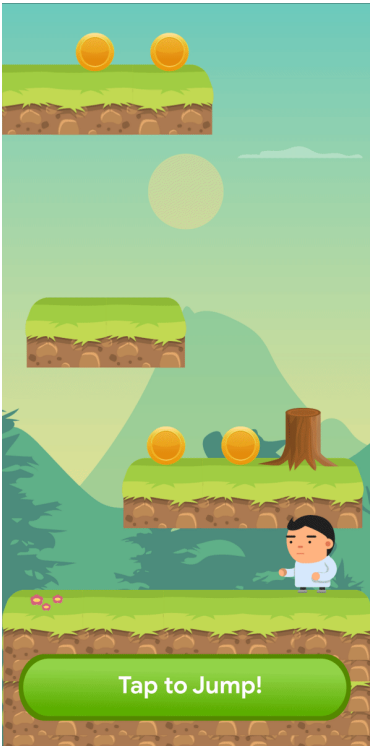


① Bu reklamın bir kapat düğmesi yoktur.

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

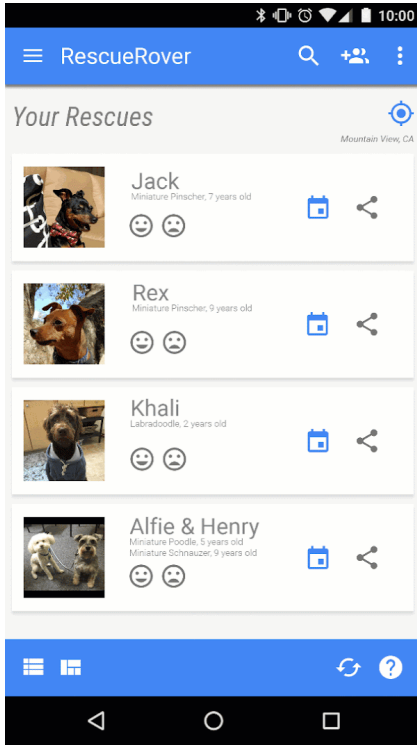


① Bu reklamda sahte kapatma düğmesi kullanılıyor.



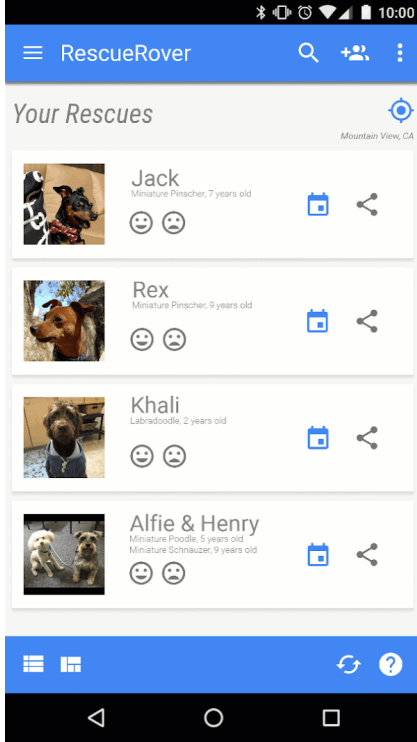
② Bu reklam, kullanıcının uygulama içi işlevler için dokunmaya alışkın olduğu bir alanda aniden görünüyor.

- Sunumu yapan uygulamanın dışında görüntülenen reklamlar:



① 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.



① Kullanıcı uygulamadan çıkmayı ve ana ekrana gitmeyi dener, ancak bunun yerine bir reklam görünür ve beklenen akış kesintiye uğrar.

Daha İyi Reklam Deneyimleri

Geliştiriciler, Google Play uygulamalarının kullanıcılarına yüksek kaliteli deneyimler sunmak için aşağıdaki reklam yönergelerine uymakla yükümlüdür. Reklamlarınız kullanıcılara aşağıdaki gibi beklenmedik şekillerde gösterilemez:

- Genellikle kullanıcı başka bir şey yapmak istediğinde beklenmedik bir şekilde ortaya çıkan hiçbir tam ekran geçiş reklamına (video, GIF, sabit vb.) izin verilmez.
- Oyun esnasında seviyenin başında veya bir içerik segmentinin başlangıcında gösterilen reklamlara izin verilmez.
- Bir uygulamanın yükleme ekranı (başlangıç ekranı) açılmadan önce tam ekran video halinde gösterilen geçiş reklamlarına izin verilmez.
- 15 saniye sonra kapatılamayan hiçbir tam ekran geçiş reklamına izin verilmez. Etkinleştirme için gösterilen veya kullanıcı işlemlerini engellemeyen (ör. bir oyun uygulamasında skor ekranından sonra görünen) tam ekran geçiş reklamları 15 saniyeden daha uzun bir süre boyunca ekranda kalabilir.

Bu politika, kullanıcılar tarafından açıkça etkinleştirilen ödüllü reklamlar (ör. geliştiricilerin belirli bir oyun özelliğinin veya içeriğin kilidini açma karşılığında kullanıcılara izlemeleri için açıkça teklifte bulunduğu reklamlar) için geçerli değildir. Bu politika, normal uygulama kullanımını veya oyun oynamayı engellemeyen reklamlar ve para kazanma yöntemleri (ör. reklamların entegre edildiği video içerikleri, tam ekran olmayan banner reklamlar) için de geçerli değildir.

Bu yönergeler, [Better Ads Standartları - Mobil Uygulama Deneyimleri](#) yönergelerinden esinlenilerek hazırlanmıştır. Better Ads Standartları hakkında daha fazla bilgi için lütfen [Coalition for Better Ads](#) sayfasına bakın.

Yaygın görülen ihlallere ilişkin bazı örnekleri aşağıda bulabilirsiniz:

- Oyun esnasında veya bir içerik segmentinin başlangıcında beklenmedik şekilde ortaya çıkan reklamlar (ör. kullanıcı bir düğmeyi tıkladıktan sonra ve düğmenin tıklanmasıyla yapılmak istenen işlem gerçekleşmeden önce) Kullanıcılar oyuna başlamayı veya içerikle etkileşime girmeyi beklediklerinden bu reklamlar beklenmedik kategorisine girer.

① Oyun esnasında seviyenin başlangıcında beklenmedik bir statik reklam gösteriliyor.

- ② İerik segmentinin bařlangıcında beklenmedik bir video reklam gsteriliyor.
- Oyun esnasında grntlenen ve 15 saniye sonra kapatılamayan tam ekran reklam

① Oyun esnasında bir geiř reklamı grntleniyor ve kullanıcılara 15 saniye iinde reklamı atlama seeneėi sunulmuyor.

Reklamlar iin retilen

Srekli olarak geiř reklamları grntleyerek kullanıcıların uygulamayı kullanmalarını ve uygulama ii grevleri yerine getirmelerini engelleyen uygulamalara izin verilmez.

Yaygın grlen ihlallere iliřkin bazı rnekleri ařaėıda bulabilirsiniz:

- Tıklamalar ve kaydırmalar da dahil ancak bunlarla sınırlı olmamak üzere her kullanıcı işleminden sonra bir geiş reklamının gösterildiđi uygulamalar

① Uygulama içindeki ilk sayfada tıklanabilecek birçok düğme var. Kullanıcı, uygulamayı kullanmak için **Start app**'i tıkladığında bir geiş reklamı görüntüleniyor. Reklam kapatıldıktan sonra kullanıcı hizmeti kullanmaya başlamak için uygulamaya dönüp **Service**'i tıklıyor ancak bu sefer başka bir geiş reklamı görüntüleniyor.

② Kullanıcı, uygulamayı kullanmak için ilk sayfadaki tek düğme olan **Play**'i tıklamaya yönlendiriliyor. Kullanıcı bu düğmeyi tıkladığında bir geiş reklamı görüntüleniyor. Reklam kapatıldıktan sonra kullanıcı sayfadaki tek düğme olan **Launch**'u tıklıyor ve başka bir geiş reklamı görüntüleniyor.

Kilitli Ekrandan Para Kazanma

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

Reklam Sahtekarlığı

Reklam sahtekarlığı kesinlikle yasaktır. Daha fazla bilgi için [Reklam Sahtekarlığı Politikamıza](#) bakabilirsiniz.

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.

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 kimliği (AAID) 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 kimliği tanımlayabilecek bilgilerle ilişkilendirilebilir.
 - Analiz için kullanım: Reklam kimliği, analiz için hiçbir şekilde kimliği tanımlayabilecek bilgilerle bağlantılı hale getirilemez veya kalıcı cihaz tanımlayıcılarla (ör. SSAID, MAC adresi, IMEI vb.) ilişkilendirilemez. Lütfen kalıcı cihaz tanımlayıcılarıyla ilgili ek yönergeler hakkında bilgi edinmek için [Kullanıcı Verileri politikasını](#) okuyun.
- **Kullanıcıların seçimlerine saygı.**
 - Sıfırlanırsa kullanıcının açık izni olmadan yeni bir reklam kimliği bir önceki reklam kimliğiyle veya önceki reklam kimliğinden 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 kimliğini kullanamazsınız. İzin verilen etkinlikler; içeriğe dayalı reklamcılık, sıklık sınırı, dönüşüm izleme, rapor gönderme, güvenlik ve sahtekarlık algılamasını içerir.
 - Kullanıcı, daha yeni cihazlarda Android reklam kimliğini sildiğinde bu kimlik kaldırılır. Kimliğe erişme girişimleri, sıfırlardan oluşan bir dize alır. Reklam kimliği olmayan bir cihaz, önceki reklam kimliğine bağlı veya bundan türetilen verilerle ilişkilendirilmemelidir.
- **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 kimliği sadece Google Play Geliştirici Program Politikaları'na 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.

Daha fazla bilgi için [Kullanıcı Verileri Politikamıza](#) bakabilirsiniz.

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. Kullanıcıları yanıltıcı veya manipülatif satın alma deneyimlerine (uygulama içi satın alma işlemleri veya abonelikler dahil) maruz bırakan uygulamalara izin verilmez.

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.

Abonelikler, kullanıcılara abonelik süresince kesintisiz veya yinelenen bir değer sunmalıdır. Kullanıcılara efektif olarak tek seferlik avantajlar (örneğin, tek kullanımlık oyun takviyeleri veya toplu halde uygulama içi krediler/para birimleri sağlayan SKU'lar) sunmak için kullanılamazlar. Aboneliğinizde teşvik veya tanıtım bonusları sunabilirsiniz. Ancak bunlar abonelik süresince kesintisiz veya yinelenen bir şekilde sunulan değeri tamamlayıcı nitelikte olmalıdır. Kesintisiz ve yinelenen değer sunmayan ürünler [abonelik ürünü](#) değil, [uygulama içi ürün](#) kullanmalıdır.

Tek seferlik avantajları abonelik gibi göstererek kullanıcılara yanlış bir şekilde tanıtamazsınız. Kullanıcı satın aldıktan sonra aboneliği değiştirerek tek seferlik teklif haline getirmek (örneğin, yinelenen değeri iptal etmek, kullanımdan kaldırmak veya en aza indirmek) bu kapsamda yer alır.

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.
- Eksiksiz bir şekilde yerleştirilmeyen 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" veya "Premium üyeliği 3 gün boyunca ücretsiz olarak deneyin" gibi ibarelerin kullanılması.
- Satın alma sürecinde, kullanıcıları abone olma düğmesini yanlışlıkla tıklamaya yönlendiren birden fazla ekran.
- Kesintisiz veya yinelenen değer sunmayan abonelikler (örneğin, aboneliğin ilk ayında 1.000 mücevher sunarken sonraki aylarında bunu 1 mücevhere düşürmek).
- Tek seferlik avantaj sunmak için kullanıcının otomatik yenilenen aboneliğe kaydolmasını şart koşturmak ve satın alma işleminden sonra kullanıcının isteği olmadan aboneliğini iptal etmek.

1. Örnek:

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 anlayabilmesi için teklifin, şartlar ve koşullar ile aynı dilde yerelleştirilmesi gerekir.

2. Örnek:

① Aynı düğme alanının tekrar tekrar tıklanmasının, kullanıcının abone olmak için sondaki "devam" düğmesini yanlışlıkla tıklamasına yol açması.

② Deneme süresinin sonunda kullanıcıdan alınacak ödeme tutarının okunaklı olmaması nedeniyle kullanıcıda planın ücretsiz olduğu izleniminin oluşabilmesi.

Ücretsiz Denemeler ve Tanıtım Amaçlı Teklifler

Kullanıcılar aboneliğinize 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.
- Eksiksiz bir şekilde yerelleştirilmeyen teklif fiyatlandırması ve şartları.

- ① Kapatma düğmesinin net bir şekilde görünmemesi ve kullanıcıların ücretsiz denemeye kaydolmadan işlemlere 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, İptal ve Geri Ödemeler

Uygulamalarınızda abonelik satıyorsanız kullanıcıların aboneliklerini nasıl yönetebilecekleri veya iptal edebilecekleri, uygulamalarınızda açıkça belirtilmelidir. Uygulamanızda, abonelik iptali için kullanıcıyı kolay online bir yöntemle erişim imkanı da sunulmalıdır. Uygulamanızın hesap ayarlarında (veya buna eşdeğer sayfada) aşağıda belirtilen öğeleri ekleyerek bu şartı yerine getirebilirsiniz:

- Google Play'in Abonelik Merkezi'nin bağlantısı (Google Play'in faturalandırma sistemini kullanan uygulamalar için) ve/veya
- İptal işleminize doğrudan erişim

Bir kullanıcı, Google Play'in faturalandırma sistemini kullanarak satın aldığı bir aboneliği iptal ederse genel politikamıza göre geçerli fatura dönemi için geri ödeme alamaz ancak iptal tarihine bakılmaksızın geçerli fatura döneminin geri kalan kısmında ilgili abonelik içeriğini almaya devam eder. Kullanıcının iptal isteği, geçerli fatura dönemi geçtikten sonra yürürlüğe girer.

Bununla birlikte siz (içerik veya erişim sağlayıcısı olarak) doğrudan kullanıcılarınız için daha esnek bir geri ödeme politikası uygulayabilirsiniz. Kullanıcılarınıza abonelik, iptal ve geri ödeme politikalarınızda değişiklikleri bildirme ve politikaların geçerli yasalara uygun olmasını sağlama konusunda sorumluluk size aittir.

Aileler İçin İçerik Üretici Onaylı Reklam SDK'sı Programı

Uygulamanızda reklam yayınlıyorsanız ve uygulamanızın hedef kitlesi, [Aile Politikası](#) 'nda açıklandığı gibi yalnızca çocukları içeriyorsa aşağıdaki Aileler İçin İçerik Üretici Onaylı Reklam SDK'sı şartları da dahil olmak üzere, yalnızca Google Play politikalarına içerik üretici onayı açısından uygun reklam SDK'sı sürümlerini kullanmanız gerekir.

Uygulamanızın hedef kitlesi hem çocukları hem de yaşça daha büyük kullanıcıları içeriyorsa çocuklara gösterilen reklamların yalnızca içerik üretici onaylı reklam SDK'sından geldiğinden emin olmanız gerekir (ör. yönlendirmesiz yaş seçim ekranı önlemlerini uygulayarak).

İçerik üretici onaylı reklam SDK sürümleri de dahil olmak üzere uygulamanızda kullandığınız tüm SDK sürümlerinin geçerli tüm politikalara, yerel yasalara ve yönetmeliklere uygun olmasını sağlama sorumluluğu size aittir. Google, reklam SDK'larının içerik üretici onayı alma sürecinde sağladıkları bilgilerin doğruluğu konusunda herhangi bir beyanda bulunmaz veya garanti vermez.

Aileler İçin İçerik Üretici Onaylı Reklam SDK'larının kullanımı yalnızca çocuklara reklam sunmak için reklam SDK'sı kullanıyorsanız 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 uygun olmasını sağlamak sizin sorumluluğunuzdadır:

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

Aileler İçin İçerik Üretici Onaylı Reklam SDK'sı Şartları

- Sakıncalı reklam içeriğini ve davranışlarını tanımlayıp bunları reklam SDK'sının şartları veya politikalarında yasaklayın. Tanımlar Google Play 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'ın 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 Google Play'in [Aile Reklamları ve Para Kazanma politikasına](#) uygun reklam biçimleri seçmesine ve [Öğretmen Onaylı programının](#) şartlarını yerine getirmesine izin verin.
- Çocuklara reklam yayınlamak için gerçek zamanlı teklif verme seçeneğini kullanırken reklam öğelerinin incelendiğinden ve gizlilik göstergelerinin teklif verenlere iletildiğinden emin olun.
- Reklam SDK'sının tüm içerik üretici onayı şartlarına uyduğunu doğrulamak için Google'a yeterli bilgi sağlayın (ör. test uygulaması ve aşağıdaki [talep formunda](#) yer alan bilgileri göndermek) ve daha sonra gönderilecek bilgi isteklerine zamanında yanıt verin (ör. reklam SDK'sı sürümünün tüm içerik üretici onayı şartlarına uyduğunu doğrulamak için yeni sürümler göndermek).
- Tüm yeni sürümlerin, Aile Politikası şartları da dahil olmak üzere en güncel Google Play Geliştirici Program Politikaları'na uygun olduğunu göstermek için [içerik üretici onayı](#) alın.

Not: Aileler İçin İçerik Üretici Onaylı Reklam SDK'ları, yayıncıları için geçerli olabilecek, çocuklarla ilgili tüm mevzuatlara ve tüzüklere uygun reklam sunmayı desteklemelidir.

Reklam öğelerine filigran ekleme ve test uygulaması sağlama hakkında daha fazla bilgiyi [burada](#) bulabilirsiniz.

Çocuklara reklam sunarken reklam sunma platformları için uyumlulaştırma şartları:

- Yalnızca Aileler İçin İçerik Üretici Onaylı Reklam SDK'larını kullanın veya uyumlulaştırma ağlarından sunulan tüm reklamların bu şartlara uymasını sağlamak için gerekli güvenlik önlemlerini uygulayın ve
- Reklam içeriği değerlendirmesini ve çocuklara yönelik olarak geçerli değerlendirmeleri belirtmek için uyumlulaştırma platformlarına gereken bilgileri sağlayın.

Geliştiriciler [burada](#) Aileler İçin İçerik Üretici Onaylı Reklam SDK'larının listesini bulabilir ve bu reklam SDK'larının hangi sürümlerinin Aileler İçin programına kayıtlı uygulamalarda kullanılmak üzere içerik üretici onayı aldığını kontrol edebilirler.

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

Mağaza Girişi ve Tanıtım

Uygulamanızın tanıtımı ve görünürlüğü mağazanın kalitesini önemli ölçüde etkiler. Spam barındıran 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. Tanıtım uygulamalarının davranışları ya da içerikleri Geliştirici Program Politikalarımızı ihlal ediyorsa bunlar aldatıcı veya zararlı olarak kabul edilir.

Yaygın görülen ihlallere ilişkin bazı örnekleri aşağıda bulabilirsiniz:

- Sistem bildirimleri ve uyarılarına benzeyen bildirimler de dahil olmak üzere, web sitelerinde, uygulamalarda veya diğer mülklerde [yanıltıcı](#) reklamlar kullanma
- Kullanıcıları uygulamanızın Google Play girişine yönlendirip uygulamanızı indirmelerini sağlamak için [müstehtecen](#) 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
- Uygulama başlığı, simgesi veya geliştirici adında, mağazadaki performansı veya sıralamayı, fiyatı ya da tanıtım amaçlı bilgileri içeren veya mevcut Google Play programlarıyla ilişkiyi çağrıştıran metin veya resim

Uygulamanızla ilişkili tüm reklam ağları, satış ortakları veya reklamların bu politikalara uymasını sağlamak sizin sorumluluğunuzdadır.

Meta veri

Uygulama açıklaması, kullanıcıların uygulamanızın işlevini ve amacını anlamalarına yardımcı olur. 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.

Uygulama başlığınız, simgeniz ve geliştirici adınız, kullanıcıların uygulamanızı bulup hakkında bilgi edinmesi için faydalıdır. Bu meta veri öğelerinde emojiler, ifadeler veya tekrarlanan özel karakterler kullanmayın. Marka adınızda yoksa BÜYÜK HARFLERLE yazmaktan kaçının. Uygulama simgelerinde yanıltıcı sembollere izin verilmez. Örneğin: yeni mesaj olmamasına rağmen yeni mesaj olduğuna dair nokta göstergesi ve uygulamanın içerik indirmeye ilgisi olmamasına rağmen indirme/yükleme simgeleri. Uygulama başlığınız 30 karakterden uzun olmamalıdır. Uygulama başlığı, simgesi veya geliştirici adında, mağazadaki performansı veya sıralamayı, fiyatı ya da tanıtım amaçlı bilgileri içeren veya mevcut Google Play programlarıyla ilişkiyi çağrıştıran metin veya resim kullanmayın.

Burada belirtilen şartlara ek olarak, bazı Google 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

- ① Marka adında olmamasına rağmen BÜYÜK HARF kullanılması
- ② Uygulamayla alakasız özel karakter dizileri
- ③ Emojilerin, ifadelerin (kaomojiler dahil) ve özel karakterlerin kullanılması
- ④ Yanıltıcı sembol
- ⑤ Yanıltıcı metin

- "Yılın Uygulaması", "1 numara", "Play'in En İyileri 20XX", "Popüler", ödül simgeleri gibi mağaza performansını veya sıralamasını belirten metin ya da resimler.

- "%10 indirim", "50 TL nakit geri ödeme", "yalnızca sınırlı süre için ücretsiz" gibi fiyat ve promosyon bilgilerini belirten metin veya resimler.

- "Editörün seçimi" veya "Yeni" gibi Google Play programlarını belirten metin ya da resimler.

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 küfür, 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.

Aşağıda, en iyi uygulamalardan birkaçını 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 kaçının.
 - 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 kaçının ve yukarıdaki kurallara uyun.
-

Kullanıcı Puanları, Yorumlar ve Yüklemler

Geliştiriciler, Google Play'deki hiçbir uygulamanın yerleşimini hileli bir şekilde değiştirmeyi denememelidir. Bu kural, sahte veya teşvik yoluyla elde edilen yorumlar ve puanlar gibi kural dışı yöntemlere başvurarak ürünün puanını yükseltme, yorumlarını şişirme veya yükleme sayılarını artırmayı ya da kullanıcıları, uygulamanın ana işlevi olarak başka uygulamaları yüklemeye teşvik etmeyi 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.

- Bir uygulamanın Google Play'deki yerleşimini etkilemek için kullanıcı kimliğine bürünüp sürekli puan verme
- 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 teklif ederek kullanıcıları RescueRover uygulamasını tanıtmaya teşvik eder.

Kullanıcı oyları ve yorumlar, uygulamanın kalitesini gösteren karşılaştırma ölçütleridir. Kullanıcılar, bu bilgilerin orijinal ve alakalı olmasına güvenir. Kullanıcı yorumlarına yanıt verirken izleyebileceğiniz birkaç en iyi uygulamayı aşağıda 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 kullanıcılarailetmesine 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. İçerik derecelendirmesi olmayan uygulamalar Play Store'dan kaldırılır.

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.

Haber

Aşağıdaki özellikleri taşıyan uygulamalar haber uygulaması olarak kabul edilir:

- Google Play Console'da kendini "haber" uygulaması olarak tanımlayan veya
- Google Play Store'da kendini "Haber ve Dergi" kategorisinde listeleyen ve uygulama başlığı, simgesi, geliştirici adı veya açıklamasında kendini "haber" olarak tanımlayan.

"Haber ve Dergi" kategorisinde yer alıp haber uygulaması olarak kabul edilen uygulamalara örnekler:

- Aşağıdakiler dahil ancak bunlarla sınırlı olmamak üzere, uygulama açıklamalarında kendilerini "haber" uygulaması olarak tanımlayan uygulamalar:
 - Son haberler
 - Gazete
 - Flaş haber
 - Yerel haberler
 - Günlük haberler
- Uygulama başlığında, simgesinde veya geliştirici adında "haber" kelimesi geçen uygulamalar.

Ancak çoğunlukla kullanıcı tarafından oluşturulan içerik barındıran uygulamalar (ör. sosyal medya uygulamaları) kendilerini haber uygulaması olarak tanımlamamalıdır. Bu uygulamalar haber uygulaması olarak kabul edilmez.

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

Haber uygulamaları şunları yapmalıdır:

- Her haber makalesinin orijinal yayıncısı veya yazarı dahil ancak bunlarla sınırlı olmamak üzere, makalelerinin kaynağı ve uygulama hakkında sahiplik bilgileri sağlamalıdır. Makale yazarlarının tek tek listelenmediği durumlarda haber uygulaması, makalelerin orijinal yayıncısı olmalıdır. Sosyal medya hesaplarına ait bağlantıların, yazar veya yayıncı bilgileri için yeterli bir kaynak olmadığını lütfen unutmayın.
- İletişim bilgileri içerdiği yönünde açıkça etiketlenmiş, kolay bulunabilen (ör. ana sayfanın altında veya sitenin gezinme çubuğunda bağlantısı olan) ve bir iletişim e-posta adresi ya da telefon numarası içerecek şekilde haber yayıncısının geçerli iletişim bilgilerini sağlayan, bu amaç için yapılmış bir web sitesi veya uygulama içi sayfaya sahip olmalıdır. Sosyal medya hesaplarına verilen bağlantıların yeterli bir yayıncı iletişim bilgisi biçimi olmadığını lütfen unutmayın.

Haber uygulamaları şunları yapmamalıdır:

- Önemli düzeyde yazım ve dil bilgisi hataları içermemeli,
- Yalnızca statik içerik (ör. üç aydan daha eski içerik) barındırmamalı veya
- Birincil amacı satış ortaklığı pazarlaması yapmak ya da reklam geliri elde etmek olmamalıdır.

Birincil amaçları ürün veya hizmet satmak ya da reklamcılık geliri oluşturmak olmadığı sürece haber uygulamalarının reklam veya başka pazarlama yollarını para kazanmak için *kullanabileceklerini* lütfen unutmayın.

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

Gerekli bilgileri en iyi nasıl sağlayacağınızı öğrenmek için lütfen [bu makaleye göz atın](#) .

Spam, İşlevsellik ve Kullanıcı Deneyimi

Uygulamalar, kullanıcılara etkileşime girebilecekleri bir deneyim sunmak için temel düzeyde uygun bir işlevsellik ve içerik sağlamalıdır. Kilitlenen, işlevsel bir kullanıcı deneyimine aykırı başka davranışlar sergileyen veya yalnızca kullanıcılara ya da Google Play'e spam yapmaya yarayan uygulamalar, katalogu 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 vermeyiz.

İleti Spam'ı

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

Aşağıda, yaygın görülen bir ihlale ilişkin örneği bulabilirsiniz:

- Kullanıcı "Paylaş" düğmesine bastığında uygulama, içeriğini ve gönderilecek alıcıları kullanıcının onaylamasına olanak sağlamadan kullanıcının adına mesajlar gönderir:

Web Görünümleri 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 vermeyiz.

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 görüntülemesini sağlamak olan uygulamalar:

① ① "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 vermeyiz. 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 oluşturmayı düşünmelidir.

İşlevsellik, İçerik ve Kullanıcı Deneyimi

Uygulamalar kararlı, duyarlı ve ilgi çekici bir kullanıcı deneyimi sunmalıdır. Kilitlenen uygulamalar, mobil uygulama olarak temel düzeyde yeterli fayda sunmayan, ilgi çekici içerik barındırmayan ya da işlevsel ve ilgi çekici bir kullanıcı deneyimine uygun olmayan başka davranışlar sergileyen uygulamalara Google Play'de izin verilmez.

Sınırlı İşlevsellik ve İçerik

Yalnızca sınırlı işlevlere ve içeriğe sahip uygulamalara izin verilmez.

Aşağıda, yaygın görülen bir ihlale ilişkin örneği bulabilirsiniz:

- Yalnızca metin veya PDF dosyası uygulamaları gibi uygulamaya özel işlevleri olmayan statik uygulamalar
- Çok az içerik barındıran ve ilgi çekici bir kullanıcı deneyimi sunmayan uygulamalar. Örneğin tek bir duvar kağıdından oluşan uygulamalar

- 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 politikalardan 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 etmeleri gerekir.

Bağlantı Desteği

Android Hazır Uygulama geliştiricilerinin diğer uygulamalarla ilgili bağlantıları doğru şekilde desteklemeleri gerekir. Geliştiricinin hazır uygulamaları veya yüklü uygulamaları, 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. [Herkes 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 şifrelenmelidir.

Android Emoji Politikası

Emoji politikamız, kapsayıcı ve tutarlı bir kullanıcı deneyimini destekleyecek şekilde tasarlanmıştır. Bunu sağlamak için tüm uygulamalar Android 12 ve sonraki sürümlerde çalışırken [Unicode Emoji](#) 'nin en son sürümünü desteklemelidir.

Herhangi bir özel uygulama içermeyen varsayılan Android Emoji'yi kullanan uygulamalar Android 12 ve sonraki sürümlerde çalışırken zaten Unicode Emoji'nin en son sürümünü kullanır.

Üçüncü taraf kitaplıkların sağladıkları da dahil olmak üzere özel emoji uygulamaları içeren uygulamalar Android 12 ve sonraki sürümlerde çalışırken, yeni Unicode Emoji kullanıma sunulduktan sonra 4 ay içinde en son Unicode sürümünü tamamen desteklemelidir.

Modern emoji'leri nasıl destekleyeceğinizi öğrenmek için bu [kılavuzu](#) inceleyin.

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.](#)

Google Play Aile Politikaları

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, uygulamanızın aileler de dahil olmak üzere tüm kullanıcılar için güvenli olduğundan 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.

Google Play Aile Politikası'na uyan tüm uygulamalar [Öğretmen Onaylı programı](#) için derecelendirilmek üzere başvurabilir ancak uygulamanızın Öğretmen Onaylı programına dahil edileceğini garanti edemeyiz.

Play Console Şartları

Hedef Kitle ve İçerik

Uygulamanızı yayınlamadan önce, Google Play Console'un [Hedef Kitle ve İçerik](#) bölümünde belirtilen yaş grupları arasından seçim yaparak uygulamanızın hedef kitlesini 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.

Uygulamanızın hedef kitlesi için birden fazla yaş grubunu yalnızca, uygulamayı seçilen yaş gruplarındaki kullanıcılar için tasarladıysanız ve uygulamanın bu kullanıcılara uygun olduğundan eminseniz 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. Uygulamanız tüm dünya için uygun olmayan ancak belirli bir bölgedeki çocuk kullanıcılar için uygun kabul edilen içerikler barındırıyor olabilir. Bu durumda uygulamanız o bölgede ([sınırlı bölgeler](#)) kullanıma sunulmaya devam ederken diğer bölgelerdeki kullanıcılar tarafından kullanılamaz.
- Uygulama işlevselliği:** Uygulamanızın tek işlevi bir web sitesinin web görünümünü sağlamak veya birincil amacı, sahibinin ya da yöneticisinin izni olmadan bir web sitesine satış ortağı trafiği çekmek olmamalıdır.
- Play Console yanıtları:** Play Console'da uygulamanızla ilgili sorulara doğru yanıtlar vermeniz ve bu yanıtları uygulamanızda yapılacak herhangi bir değişikliği doğru yansıtacak şekilde güncellemeniz gerekir. Buna, Hedef Kitle ve İçerik bölümünde, Veri Güvenliği bölümünde ve IARC İçerik Derecelendirme Anketi'nde uygulamanızla ilgili doğru yanıtlar vermek dahildir ancak bununla sınırlı değildir.
- Veri uygulamaları:** Uygulamanızda çocuklara ait [kişisel ve hassas bilgilerin](#) toplanıp toplanmadığını belirtmelisiniz. 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 de dahil ancak bunlarla sınırlı olmayan bilgiler, çocuklardan toplanan hassas bilgiler kapsamına girer. Ayrıca uygulamanızın aşağıdaki [veri uygulamalarına](#) uyduğundan da emin olmanız gerekir:
 - Yalnızca çocukları hedefleyen uygulamalar; Android reklam kimliği (AAID), SIM Seri Numarası, Derleme Seri Numarası, BSSID, MAC, SSID, IMEI ve/veya IMSI numarasını aktarmamalıdır.
 - Yalnızca çocukları hedefleyen uygulamalar, Android API 33 veya sonraki sürümleri hedeflerken AD_ID izni istememelidir.
 - Hem çocukları hem de yaşça daha büyük kitleleri hedefleyen uygulamalar, çocuklardan veya yaşı bilinmeyen kullanıcılardan AAID, SIM Seri Numarası, Derleme Seri Numarası, BSSID, MAC, SSID, IMEI ve/veya IMSI numarasını aktarmamalıdır.
 - Cihazın telefon numarası Android API TelephonyManager'dan istenmemelidir.
 - Yalnızca çocukları hedefleyen uygulamalar konum izni isteyemez veya [tam konum](#) bilgisi toplayamaz, kullanamaz ve iletemez.
 - Bluetooth kullanımı isteğinde bulunan uygulamalar [Companion Device Manager'ı \(CDM\)](#) kullanmalıdır (uygulamanız yalnızca CDM ile uyumlu olmayan cihaz işletim sistemi (OS) sürümlerini hedeflemiyorsa).
- API'ler ve SDK'lar:** Uygulamanızın API'leri ve SDK'ları doğru bir şekilde uyguladığından emin olmalısınız.
 - Yalnızca çocukları hedefleyen uygulamalar, birincil olarak çocuklara yönelik hizmetlerde kullanımı onaylanmamış API'leri veya SDK'ları içermemelidir.
 - Kimlik doğrulama ve yetkilendirme için OAuth teknolojisini kullanan ve hizmet şartlarında, çocuklara yönelik hizmetlerde kullanıma uygun olmadığı belirtilen API hizmetleri buna örnek gösterilebilir.
 - 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 [yönlendirmesiz yaş seçim ekranı](#) işlevinin arkasında kullanılması veya çocuklardan veri toplanmasına 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 uygulama içeriğine erişmesini gerektirmemelidir.

6. **Artırılmış Gerçeklik (AR):** 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 (örneğin Daydream, Oculus) kullanılmasını gerektirmemelidir.

7. **Sosyal Uygulamalar ve Özellikler:** Uygulamanızda bilgi paylaşımına veya alışverişine izin veriliyorsa bu özellikleri Play Console'daki [İçerik Derecelendirmesi Anketi](#)'nde doğru bir şekilde açıklamanız gerekir.

- Sosyal Uygulamalar: Sosyal uygulamalar, kullanıcıların serbest biçimli içerikler paylaşmasını veya büyük kullanıcı gruplarıyla iletişim kurmasını sağlamanın ana odak noktası olduğu uygulamalardır. Hedef kitlesinde çocukların yer aldığı tüm sosyal uygulamalar, çocuk kullanıcıların serbest biçimli medya içeriği veya bilgi alışverişinde bulunmasına izin vermeden önce uygulama içinde bir hatırlatma görüntülemelidir. Bu hatırlatmada, internette güvenliği elden bırakmamaları ve internetteki etkileşimin gerçek dünyadaki risklerinin farkında olmaları gerektiği vurgulanmalıdır. Ayrıca çocuk kullanıcıların kişisel bilgi alışverişinde bulunmasına izin vermeden önce, bir yetişkin tarafından işlem yapılması zorunlu tutulmalıdır.
- Sosyal Özellikler: Sosyal özellikler, kullanıcıların serbest biçimli içerik paylaşmasını veya büyük kullanıcı gruplarıyla iletişim kurmasını sağlayan ilave uygulama işlevsellikleridir. Hedef kitlesinde çocukların yer aldığı ve sosyal özellikler içeren tüm uygulamalar, çocuk kullanıcıların serbest biçimli medya içeriği veya bilgi alışverişinde bulunmasına izin vermeden önce uygulama içinde bir hatırlatma görüntülemelidir. Bu hatırlatmada, internette güvenliği elden bırakmamaları ve internetteki etkileşimin gerçek dünyadaki risklerinin farkında olmaları gerektiği vurgulanmalıdır. Ayrıca yetişkinlere, sosyal özelliği etkinleştirme/devre dışı bırakma veya farklı işlevsellik seviyeleri seçme dahil ancak bunlarla sınırlı olmamak üzere çocuk kullanıcılar için sosyal özellikleri yönetebilecekleri bir yöntem sunulmalıdır. Son olarak, çocukların kişisel bilgi alışverişinde bulunmasına izin veren özellikler etkinleştirilmeden önce yetişkinler tarafından işlem yapılması zorunlu tutulmalıdır.
- Yetişkinler tarafından yapılan işlem, kullanıcının çocuk olmadığını ve çocukları, uygulamanızın yetişkinler için tasarlanmış bölümlerine erişebilmek amacıyla yaşları hakkında yanlış bilgi vermeye teşvik etmediğini doğrulamaya yarayan bir mekanizmadır (ör. yetişkin PIN'i, şifre, doğum tarihi, e-posta doğrulaması, fotoğraflı kimlik, kredi kartı veya SSN).
- Ana odak noktası yabancılarla sohbet etmek olan sosyal uygulamalar, çocukları hedeflememelidir. Chat roulette tarzı uygulamalar, flört uygulamaları, çocuk odaklı açık sohbet odaları vb. buna örnek gösterilebilir.

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 Politikaları](#) 'nı ihlal eden içeriğe sahip web sitelerine bağlantılar içeren uygulamalar.
- Yetişkinlere yönelik reklamları (ör. şiddet barındıran içerik, cinsel içerik, kumar içeriği) çocuklara gösteren uygulamalar.

Reklamlar ve Para Kazanma

Play'de çocukları hedefleyen bir uygulamadan para kazanıyorsanız uygulamanızın Aile Reklamları ve Para Kazanma Politikası Şartları'na uyması önemlidir.

Aşağıdaki politikalar; reklamlar, çapraz tanıtımlar (uygulamalarınız ve üçüncü taraf uygulamaları için olanlar), uygulama içi satın alma teklifleri veya her türlü ticari içerik (ör. ücretli ürün yerleşimi) de dahil olmak üzere uygulamanızdaki tüm para kazanma yöntemleri ve reklamlar için geçerlidir. Bu uygulamalardaki tüm para kazanma yöntemleri ve reklamlar (ilgili tüm özdenetimli 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 koşulları

Uygulamanız çocuklara veya yaşı bilinmeyen kullanıcılara reklam gösteriyorsa şunları yapmalısınız:

- Bu kullanıcılara reklam gösterirken yalnızca [Google Play Aileler İçin İçerik Üretici 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 Aileler reklam biçimiyle ilgili koşullara uyduğundan emin olmalısınız ve
- Çocuklara reklam sunmayla ilgili geçerli tüm yasal düzenlemelere ve endüstri standartlarına uymalısınız.

Reklam biçimleriyle ilgili koşullar

Uygulamanızdaki para kazanma yöntemleri ve reklamlar, yanıltıcı içerik barındırmamalı veya çocuk kullanıcıların yanlışlıkla tıklamasına yol açacak şekilde tasarlanmamalıdır.

Uygulamanızın tek hedef kitlesi çocuklarsa aşağıdakiler yasaktır. Uygulamanızın hedef kitlesinde hem çocuklar hem de yaşça daha büyük kullanıcılar varsa çocuklara veya yaşı bilinmeyen kullanıcılara reklam gösterirken aşağıdakiler yasaktır:

- Tüm ekranı kaplayan ya da normal kullanımı etkileyen ve reklamı kapatmak için açık bir yöntem sunmayan reklamlar ve para kazanma yöntemleri de dahil olmak üzere kullanımı engelleyen para kazanma yöntemleri ve reklamlar (örneğin [reklam duvarları](#))
- Normal uygulama kullanımı veya oyun oynamayı engelleyen ve 5 saniye sonra kapatılamayan para kazanma yöntemleri ve reklamlar (ödüllü veya seçime dayalı reklamlar dahil)
- Normal uygulama kullanımı veya oyun oynamayı engellemeyen reklamlar ve para kazanma yöntemleri 5 saniyeden uzun süre devam edebilir (örneğin entegre reklamlar barındıran video içeriği).
- Geçiş reklamlarının ve para kazanma yöntemlerinin, uygulama başladıktan hemen sonra görüntülenmesi
- Bir sayfada birden fazla reklam yerleşimi (örneğin 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 para kazanma yöntemleri ve reklamlar (örneğin, offerwall'lar ve diğer tam sayfa reklam deneyimleri)
- Reklamların görüntülenmesini veya uygulama içi satın alma işlemlerinin gerçekleştirilmesini teşvik etmek için sarsıcı veya duygusal açıdan manipülatif taktiklerin kullanılması
- Başka bir reklamı tetiklemek için kapatma düğmesi kullanarak veya uygulamada kullanıcıların genellikle başka bir işlev için dokunduğu alanlarda aniden reklam göstererek kullanıcıları tıklamaya zorlayan yanıltıcı reklamlar
- Uygulama içi satın alma işlemleri gerçekleştirmek için sanal oyun paraları ile gerçek para arasında ayırım sağlamama

Yaygın görülen ihlallere ilişkin bazı örnekleri aşağıda bulabilirsiniz:

- Kullanıcı kapatmaya çalışırken kullanıcının parmağından uzaklaşan reklamlar ve para kazanma yöntemleri
- Aşağıdaki örnekte gösterildiği gibi, kullanıcıya beş (5) saniyeden sonra tekliften çıkma olanağı vermeyen reklamlar ve para kazanma yöntemleri:

- Aşağıdaki örnekte gösterildiği gibi, ekranın büyük kısmını veya cihaz ekranını kaplayan ve kullanıcıya kolay bulunabilir bir kapatma yöntemi sunmayan reklamlar ve para kazanma yöntemleri:

- Birden fazla teklif gösteren, aşağıdaki gibi banner reklamlar:

- Aşağıdaki örnekte gösterildiği gibi, kullanıcının uygulama içeriğiyle karıştırılabileceği reklamlar ve para kazanma yöntemleri:

- Aşağıdaki örnekte gösterildiği gibi, diğer Google Play mağaza girişlerinizi tanıtan ancak uygulama içeriğinden ayırt edilemeyen düğmeler, reklamlar veya diğer para kazanma yöntemleri:

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.

- **Kontrole 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.
- **Flört veya İlişkiler:** Flört 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 yalnızca [aileler için içerik üretici onaylı reklam SDK'sı](#) sürümlerini kullanmanız gerekir. Uygulamanızın hedef kitlesi hem çocukları hem de yaşça daha büyük kullanıcıları içeriyorsa [yönlendirmesiz yaş seçim ekranı](#) gibi yaş filtreleme önlemleri uygulayarak çocuklara gösterilen reklamların yalnızca aileler için içerik üretici onaylı reklam SDK'larından geldiğinden emin olmanız gerekir.

Bu şartlar hakkında daha fazla bilgi edinmek isterseniz [Aileler İçin İçerik Üretici Onaylı Reklam SDK'sı Programı Politikası](#) sayfasına bakabilirsiniz. Aileler için içerik üretici onaylı reklam SDK'sı sürümlerinin güncel listesini görmek için [buraya](#) göz atabilirsiniz.

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 sağlayıcılarınızla iletişime geçin.

Aileler İçin İçerik Üretici Onaylı Reklam SDK'sı Politikası

Google Play, çocuklara ve ailelere güvenli bir deneyim sunmayı taahhüt eder. Çocukların yalnızca kendi yaşlarına uygun reklamları görmelerini ve verilerinin düzgün bir şekilde işlenmesini sağlamak bu taahhüdün önemli bir parçasıdır. Bu hedefe ulaşmak için reklam SDK'larının ve uyumlulaştırma platformlarının çocuklar için uygun olduğuna, ayrıca [Google Play Geliştirici Program Politikaları](#) 'na ve [Google Play Aile Politikası](#) 'na (Aileler İçin İçerik Üretici Onaylı Reklam SDK'sı Programı şartları dahil) uygun olduğuna dair içerik üretici onayı almalarını zorunlu kılabiliriz.

Google Play Aileler İçin İçerik Üretici Onaylı Reklam SDK'sı Programı, geliştiricilerin, çocuklar için özel olarak tasarlanmış uygulamalarda kullanılmaya uygun olduğuna dair içerik üreticisi onayı alan reklam SDK'larını veya uyumlulaştırma platformlarını tanımlamaları açısından önemlidir.

Talep formu başvurunuzdaki bilgiler de dahil olmak üzere SDK'nızla ilgili herhangi bir bilginin yanlış beyan edilmesi, SDK'nızın Aileler İçin İçerik Üretici Onaylı Reklam SDK'sı Programı'ndan kaldırılmasına veya askıya alınmasına neden olabilir. Bu nedenle doğru bilgileri sağlamanız önemlidir.

Politika şartları

SDK'nız veya uyumlulaştırma platformunuz Google Play Aileler İçin Programı kapsamındaki uygulamaları yayınlıyorsa aşağıdaki şartlar da dahil olmak üzere tüm Google Play Geliştirici Politikaları'na uymanız gerekir. Politika şartlarına uyulmaması, Aileler İçin İçerik Üretici Onaylı Reklam SDK'sı Programı'ndan kaldırılmaya veya askıya alınmaya neden olabilir.

SDK'nızın veya uyumlulaştırma platformunuzun uygun olmasını sağlamak sizin sorumluluğunuzdadır. Bu nedenle, [Google Play Geliştirici Program Politikaları](#), [Google Play Aile Politikaları](#) ve [Aileler İçin İçerik Üretici Onaylı Reklam SDK'sı Programı şartlarını](#) mutlaka inceleyin.

1. **Reklam içeriği:** Çocukların erişebileceği reklam içeriğiniz çocuklara uygun olmalıdır.

- (i) Sakıncalı reklam içeriğini ve davranışlarını tanımlamanız ve (ii) şartlarınızda veya politikalarınızda bunları yasaklamanız gerekir. Tanımlar [Google Play Geliştirici Program Politikaları](#)'na uygun

olmalıdır.

- Ayrıca, reklam öğelerinizi yaş gruplarına uygunluğa göre derecelendirecek bir yöntem oluşturmanız gerekir. Yaş grupları arasında en azından Herkes için ve Yetişkinlere yönelik gruplar bulunmalıdır. Derecelendirme yöntemi, Google'ın [başvuru formunu](#) dolduran SDK'lara sağladığı yöntemle tutarlı olmalıdır.
 - Çocuklara reklam yayınlamak için gerçek zamanlı teklif verme seçeneğini kullanırken reklam öğelerinin incelendiğinden ve yukarıdaki şartlara uyduğundan emin olun.
 - Ayrıca, [reklam öğelerinin hangi envantere ait olduğunu görsel olarak tanımlayacak bir mekanizmanın](#) olması gerekir (ör. reklam öğesine şirketinizin görsel logosunu veya benzer işleve sahip bir öğeyi filigran olarak ekleme).
2. **Reklam biçimi:** Çocuk kullanıcılara gösterilen tüm reklamlar, aileler için reklam biçimleriyle ilgili koşullara uymalıdır. Ayrıca, geliştiricilerin [Google Play Aile Politikası](#)'na uygun reklam biçimlerini seçmelerine izin vermeniz gerekir.
- Reklamlar aldatıcı içerik barındırmamalı veya çocuk kullanıcıların yanlışlıkla tıklamasına sebep olacak şekilde tasarlanmış olmamalıdır. Başka bir reklamı tetiklemek için kapatma düğmesi kullanarak veya uygulamada kullanıcıların genellikle başka bir işlev için dokunduğu alanlarda aniden reklam göstererek kullanıcıları tıklamaya zorlayan yanıltıcı reklamlara izin verilmez.
 - Ekranın tamamını kaplayan veya normal kullanımı engelleyen ve reklamı kapatmak için açık bir yöntem sunmayan reklamlar da dahil olmak üzere kullanımı engelleyen reklamlara (ör. [reklam duvarları](#)) izin verilmez.
 - Ödüllü veya seçime dayalı reklamlar da dahil olmak üzere normal uygulama kullanımı veya oyun oynamayı engelleyen reklamlar 5 saniye sonra kapatılabilir.
 - Bir sayfaya birden fazla reklam yerleştirilmesine izin verilmez. Örneğin, bir yerleşimde birden fazla fırsat gösteren banner reklamlara veya birden fazla banner ya da video reklam göstermeye izin verilmez.
 - Reklamlar uygulama içeriğinden belirgin bir şekilde ayırt edilebilmelidir. Reklam olduğu çocuk kullanıcılar tarafından açıkça ayırt edilemeyen offerwall'lara ve tam sayfa reklam deneyimlerine izin verilmez.
 - Reklamlarda, reklamların görüntülenmesini teşvik etmek için sarsıcı veya duygusal açıdan manipülatif taktikler kullanılmamalıdır.
3. **İlgi alanına dayalı reklamcılık/yeniden pazarlama:** Çocuk kullanıcılara gösterilen reklamlarda ilgi alanına dayalı reklamcılık (internetteki 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) kullanılmamalıdır.
4. **Veri uygulamaları:** SDK sağlayıcı olarak kullanıcı verilerini (ör. cihaz bilgileri de dahil olmak üzere kullanıcıdan alınan veya kullanıcı hakkında toplanan bilgiler) nasıl kullandığınız konusunda şeffaf olmanız gerekir. Bu gereklilik, SDK'nızın verilere erişme ve onları toplama, kullanma ve paylaşma şeklinin açıklanması, ayrıca veri kullanımının açıklanan amaçlarla sınırlandırılması anlamına gelir. Bu Google Play şartları, geçerli gizlilik ve veri koruma yasalarında belirtilen şartlara ek olarak uygulanır. Çocuklara ait [kişisel ve hassas bilgilerin](#) toplanıp toplanmadığını açıklamalısınız. Kimlik doğrulama bilgileri, mikrofon ve kameraya ait sensör verileri, cihaz verileri, Android kimliği ve reklam kullanım verileri de dahil ancak bunlarla sınırlı olmayan bilgiler bu kapsama girer.
- Yayıncıların, istek bazında veya uygulama bazında reklam sunumu için çocuklara yönelik olarak değerlendirilme isteğinde bulunmalarına izin vermeniz gerekir. 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.
 - Çocuklara reklam yayınlamak için gerçek zamanlı teklif verme seçeneğini kullanırken gizlilik göstergelerinin teklif verenlere iletilmesini sağlamanız gerekir.

- Çocukların veya yaşı bilinmeyen kullanıcıların AAID, SIM Seri Numarası, Derleme Seri Numarası, BSSID, MAC, SSID, IMEI ve/veya IMSI numarasını aktarmamalısınız.
5. **Uyumlaştırma platformları:** Çocuklara reklam yayınlarken yapmanız gerekenler aşağıda belirtilmiştir:
- Yalnızca Aileler İçin İçerik Üretici Onaylı Reklam SDK'larını kullanın veya uyumlaştırma ağlarından sunulan tüm reklamların bu şartlara uymasını sağlamak için gerekli güvenlik önlemlerini uygulayın ve
 - Reklam içeriğinin derecelendirmesini ve çocuklara yönelik geçerli değerlendirmeleri belirtmek için uyumlaştırma platformlarına gereken bilgileri sağlayın.
6. **İçerik üretici onayı ve uygunluk:** Reklam SDK'sının tüm içerik üretici onayı şartlarına uyduğunu doğrulamak için Google'a aşağıdakiler dahil ancak bunlarla sınırlı olmamak üzere yeterli bilgi (ör. [talep formunda](#) yer alan bilgiler) sağlamanız gerekir:
- SDK'nızın veya uyumlaştırma platformunuzun Hizmet Şartları, Gizlilik Politikası ve Yayıncı Entegrasyonu Kılavuzu'nun İngilizce versiyonunu sağlamak
 - Reklam SDK'sının en güncel uygun sürümünü kullanan bir [örnek test uygulaması](#) göndermek. Örnek test uygulaması, SDK'nın tüm özelliklerini kullanan eksiksiz ve yürütülebilir bir Android APK'sı olmalıdır. Test uygulaması şartları:
 - Test uygulamanız bir telefon form faktöründe çalışmak üzere tasarlanmış, eksiksiz ve yürütülebilir bir Android APK'sı olarak gönderilmelidir.
 - Google Play'in politikalarına uygun nitelikteki reklam SDK'sının yayınlanan son sürümünü veya yayınlanmak üzere olan bir sürümünü kullanmalıdır.
 - Reklam SDK'nızın, reklam almak ve görüntülemek için reklam SDK'nızı çağırmak da dahil tüm özelliklerini kullanmalıdır.
 - Test uygulaması üzerinden istenen reklam öğeleri aracılığıyla ağdaki tüm yayındaki/gösterilen reklam envanterlerine tam erişime sahip olmalıdır.
 - Coğrafi konuma göre kısıtlanmamalıdır.
 - Envanteriniz karma bir kitleye yönelikse test uygulamanız tam envanterden reklam öğesi istekleri ile çocuklar veya tüm yaş grupları için uygun olan envanterden reklam öğesi isteklerini ayırt edebilecek durumda olmalıdır.
 - Yönlendirmesiz yaş seçim ekranı ile kontrol edilmediği sürece envanterdeki belirli reklamlarla kısıtlanmamalıdır.
7. Sürecin devamında istenebilecek her türlü bilgiyi vaktinde sağlamanız ve tüm yeni sürümlerin Aile Politikası şartları da dahil olmak üzere en güncel Google Play Geliştirici Program Politikaları'na uygun olduğuna dair [içerik üretici onayı](#) almanız gerekir.
8. **Yasal uygunluk:** Aileler için içerik onaylı reklam SDK'ları, yayıncıları için geçerli olabilecek, çocuklarla ilgili tüm mevzuatlara ve tüzüklere uygun reklam sunmayı desteklemelidir.
- SDK'nızın veya uyumlaştırma platformunuzun [ABD'de Çocukların Çevrimiçi Gizliliğini Koruma Yasası \(COPPA\)](#) , [AB'de Genel Veri Koruma Yönetmeliği \(GDPR\)](#) ve diğer tüm geçerli yasa ve yönetmeliklere uygunluğunu sağlamanız gerekir.

Not: "Çocuk" kelimesi farklı yerlerde ve değişik bağlamlarda farklı anlama gelebilir. Uygulamanız için geçerli olabilecek yükümlülükler ve/veya yaşa bağlı kısıtlamaları belirlemek için yasal danışmanınızdan yardım almanız önemlidir. Uygulamanızın nasıl çalıştığını en iyi siz bilirsiniz. Bu nedenle, Google Play'deki uygulamaların aileler için güvenli olmasını sağlama konusunda gereken yardımı sağlayacağınıza inanıyoruz.

[Aileler İçin İçerik Üretici Onaylı Reklam SDK'sı Programı](#) sayfasından program şartları hakkında daha fazla bilgi edinebilirsiniz.

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 kaldırıncaya 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 ayarlarınızdan 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

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

Yaptırım Süreci

İçeriklerin veya hesapların yasa dışı olup olmadıklarını ya da politikalarımızı ihlal edip etmediklerini incelerken, karar vermeden önce pek çok bilgiyi dikkate alırız. Bunlara meta veriler (örneğin, uygulama başlığı, açıklama), uygulama içi deneyim, hesap bilgileri (örneğin, geçmişteki politika ihlalleri), uygulamalardaki üçüncü taraf kodları ve kullanılabiliriyorsa bildirim sistemleri üzerinden sağlanan diğer bilgilerin yanı sıra kendi başlattığımız incelemeler dahildir. Uygulamanızda kullanılan bütün üçüncü taraf kodlarının (ör. SDK) ve bu üçüncü tarafların uygulamanızla ilgili işlemlerinin tüm Google Play Geliştirici Program Politikaları'na uymasını sağlamak sizin sorumluluğunuzdadır.

Uygulamanız veya geliştirici hesabınız politikalarımızdan herhangi birini ihlal ediyorsa aşağıda belirtildiği gibi gerekli 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 hesabınızda, uygulamanızda veya daha geniş bağlamda uygulama kataloğunuzda bulunan politika ihlallerinin hepsini belirtmeyebileceğini lütfen unutmayın. Politika sorunlarını giderme ve uygulamanın veya hesabının geri kalanının politikalarla tam olarak uyumlu olması için gereken ekstra özeni gösterme sorumluluğu geliştiricilere aittir. Hesabınızdaki ve tüm uygulamalarınızda politika ihlallerinin giderilmemesi ek yaptırım işlemlerine 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 uygulamalarınızı farklı şekillerde etkileyebilir. Politikalarımızı ihlal etmenin yanı sıra kullanıcılara ve genel olarak Google Play ekosistemine zarar veren içerikleri tespit edip değerlendirmek için uygulamaları ve uygulama içeriklerini inceleriz. İncelemelerde gerçek kişilerden ve otomatik değerlendirme modellerinden yararlanırsınız. Otomatik modelleri kullanmak, daha fazla ihlali tespit edip olası sorunları daha hızlı bir şekilde değerlendirmemizi sağlar. Bu da Google Play'in herkes için güvenli bir yer olarak kalmasını sağlamamıza yardımcı olur. Politikaları ihlal eden içerikler otomatik modellerimiz tarafından kaldırılır. Ancak daha incelikli bir karar verilmesi gereken içerikler olduğunda (örneğin, içeriğin bağlamının anlaşılması gerektiğinde), içeriği değerlendirecek eğitimli operatörler ve analistler tarafından incelenmek üzere işaretlenir. Daha sonra bu manuel incelemelerin sonuçları, makine öğrenimi modellerimizi daha fazla iyileştirmek amacıyla eğitim verilerinin derlenmesi için kullanılır.

Aşağıdaki bölümde, Google Play'in gerçekleştirebileceği çeşitli işlemler ve bunların uygulamanız ve/veya Google Play Geliştirici hesabınız üzerindeki etkisi açıklanmaktadır.

Yaptırımla ilgili iletişimlerde aksi belirtilmediği sürece bu işlemler tüm bölgelerde geçerlidir. Örneğin, askıya alınan bir uygulama hiçbir bölgede kullanılamaz. Ayrıca, aksi belirtilmediği sürece, işleme itiraz edip olumlu sonuç almadığınız takdirde bu işlemler geçerliliğini sürdürür.

Reddetme

- İnceleme için gönderilen yeni bir uygulama veya uygulama güncellemesi Google Play'de kullanıma sunulmaz.
- Mevcut bir uygulamada yapılan bir güncelleme reddedildiyse güncellemeden 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 kaldırıldığından kullanıcılar uygulamanın mağaza girişini göremezler. 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 alındığından kullanıcılar uygulamanın mağaza girişini göremezler.
- Askıya alınmış bir uygulamanın APK'sını veya uygulama paketini artık kullanamazsınız.
- Kullanıcılar uygulama içi satın alma işlemi yapamaz 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.

Sınırlı Görünürlük

- Uygulamanızın Google Play'deki bulunabilirliği kısıtlanır. Uygulamanız Google Play'de kullanıma sunulmaya devam eder ve kullanıcılar 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 görmesini etkilemez.

Sınırlı Bölgeler

- Uygulamanız yalnızca belirli bölgelerdeki kullanıcılar tarafından Google Play'den indirilebilir.
- Diğer bölgelerdeki kullanıcılar, uygulamayı Play Store'da bulamazlar.
- Uygulamayı daha önce yüklemiş olan kullanıcılar cihazlarında kullanmaya devam edebilirler ancak artık güncelleme almazlar.
- Bölge sınırlaması, Google Play Geliştirici hesabınızın durumunu etkilemez.

Hesap Kısıtlandı durumu

- Geliştirici hesabınız kısıtlandığında kataloğunuzdaki tüm uygulamalar Google Play'den kaldırılır ve artık yeni uygulama yayınlamaz veya mevcut uygulamaları tekrar yayınlamazsınız. Play Console'a erişmeye devam edebilirsiniz.
- Tüm uygulamalar kaldırıldığından kullanıcılar uygulamanızın mağaza girişini ve geliştirici profilinizi göremezler.

- Mevcut kullanıcılarınız uygulama içi satın alma işlemi yapamaz veya uygulamalarınızın uygulama içi faturalandırma özelliklerini kullanamazlar.
- Google Play'e daha fazla bilgi vermek ve hesap bilgilerinizde değişiklik yapmak için Play Console'u kullanmaya devam edebilirsiniz.
- Tüm politika ihlallerini giderdikten sonra uygulamalarınızı tekrar yayınlatabilirsiniz.

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 politika ihlalleri Play Console hesabınızın feshedilmesine de yol açabilir.
- Feshedilen hesaptaki uygulamalar kaldırıldığından kullanıcılar uygulamalarınızın mağaza girişini ve geliştirici profilinizi göremezler.
- Mevcut kullanıcılarınız uygulama içi satın alma işlemi yapamaz veya uygulamalarınızın uygulama içi faturalandırma özelliklerini kullanamazlar.

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.

Etkin Olmayan Hesaplar

Etkin olmayan hesaplar, aktif olmayan veya artık kullanılmayan geliştirici hesaplarıdır. Etkin olmayan hesaplar, [Geliştirici Dağıtım Sözleşmesi](#) uyarınca iyi durumda değildir.

Google Play Geliştirici Hesapları, uygulama yayınlayan ve bunları aktif şekilde kullanıcılara sunmaya devam eden aktif geliştiricilere yöneliktir. Etkin olmayan, kullanılmayan veya düzenli olarak kayda değer şekilde ilgilenilmeyen (örneğin, uygulama yayınlama ve güncelleme, istatistiklere erişme ya da mağaza girişlerini yönetme amacıyla) hesapları kötüye kullanımı önlemek amacıyla kapatırız.

[Etkin olmayan hesabın kapatılması](#) durumunda hesabınız ve bununla ilişkili tüm veriler silinir. Kayıt ücretiniz iade edilemez ve bu tutarı kaybedersiniz. Etkin olmayan hesabınızı kapatmadan önce bu hesap için verdiğiniz iletişim bilgilerini kullanarak sizi bilgilendiririz.

Etkin olmayan hesabınızın kapatılması, gelecekte Google Play'de uygulama yayınlamaya karar verdiğinizde yeni bir hesap oluşturmanıza engel olmaz. Hesabınızı yeniden etkinleştiremediğiniz gibi geçmiş uygulamalar veya veriler de yeni hesabınızda kullanılamaz.

Politika İhlallerini Yönetme ve Bildirme

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 uygulayabilir veya [burayı tıklayabilirsiniz](#).

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 konuda tavsiyeye ihtiyacınız varsa lütfen hukuk danışmanınıza başvurun.

- [Uygulama doğrulama](#)
 - [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](#)
-

Play Console Şartları

Google Play, canlı uygulama ekosisteminin güvenliğini sağlamak için Play Console geliştirici hesabınıza bağlı profiller de dahil olmak üzere tüm geliştiricilerin Play Console şartlarını karşılamasını zorunlu kılar. Kullanıcıların geliştiricilere güvenmesine yardımcı olmak için Google Play'de doğrulanmış bilgiler gösterilir. [Google Play'de gösterilen bilgiler](#) hakkında daha fazla bilgi edinin.

Google Play, kişisel ve kuruluş olmak üzere iki tür geliştirici hesabı sunar. Doğru geliştirici hesabını seçmeniz ve gerekli doğrulama işlemlerini tamamlamanız, sorunsuz bir ilk katılım deneyimi için oldukça önemlidir. [Geliştirici hesabı türü seçme](#) hakkında bilgi edinin.

Play Console hesabınızı oluştururken aşağıdaki hizmetleri sunan geliştiricilerin kuruluş olarak kaydolmaları gerekir:

- Bankacılık, krediler, hisse senedi alım satımı, yatırım fonları, kripto para yazılım cüzdanları ve kripto para borsaları dahil ancak bunlarla sınırlı olmamak üzere mali ürünler ve hizmetler. [Finansal Hizmetler Politikası](#) hakkında daha fazla bilgi edinin.
- Tıbbi uygulamalar ve insan deneyleri araştırma uygulamaları gibi sağlık uygulamaları. [Sağlık uygulaması kategorileri](#) hakkında daha fazla bilgi edinin.
- [VpnService](#) sınıfını kullanması onaylanan uygulamalar. [VPN Hizmet politikası](#) hakkında daha fazla bilgi edinin.
- Bir devlet kurumu tarafından veya onun adına geliştirilen uygulamalar da dahil olmak üzere resmi uygulamalar.

Hesap türü seçtikten sonra yapmanız gerekenler:

- Aşağıdakiler de dahil olmak üzere geliştirici hesabınızla ilgili doğru bilgiler verin:
 - Yasal ad ve adres
 - [D-U-N-S numarası](#) (kuruluş olarak kaydoluyorsanız)
 - İletişim e-posta adresi ve telefon numarası
 - Google Play'de gösterilen geliştirici e-posta adresi ve telefon numarası (geçerliyse)
 - Ödeme yöntemleri (geçerliyse)
 - Geliştirici hesabınıza bağlı Google ödeme profili
- Kuruluş olarak kaydoluyorsanız geliştirici hesabınızdaki bilgilerin güncel ve Dun & Bradstreet profilinizdeki bilgilerle tutarlı olduğundan emin olun.

Uygulamanızı göndermeden önce:

- Tüm uygulama bilgilerini ve meta verilerini doğru bir şekilde sağlayın.
- Uygulamanızın gizlilik politikasını yükleyin ve Veri Güvenliği bölümünde istenen bilgileri sağlayın.
- Etkin bir demo hesabı, giriş bilgileri ve uygulamanızın Google Play tarafından incelenebilmesi için gereken diğer tüm kaynakları (ör. [giriş kimlik bilgileri](#), QR kodu vb.) sağlayın.

Her zaman olduğu gibi uygulamanızın kararlı, ilgi çekici ve duyarlı bir kullanıcı deneyimi sunduğundan emin olmalısınız. Reklam ağları, analiz hizmetleri ve üçüncü taraf SDK'ları da dahil olmak üzere uygulamanızdaki her şeyin Google Play [Geliştirici Program Politikaları](#)'na uyduğunu bir kez daha kontrol

edin. Ayrıca uygulamanızın hedef kitlesi çocukları da içeriyorsa [Aile Politikası](#)'na uyduğunuzdan da emin olun.

Uygulamanızın, [Geliştirici Dağıtım Sözleşmesi](#) ve tüm [Geliştirici Program Politikaları](#)'na tam anlamıyla uyduğundan emin olmak için bu politikaları incelemenin sizin sorumluluğunuzda olduğunu unutmayın.

[Developer Distribution Agreement](#)

Daha fazla yardıma mı ihtiyacınız var?

Bir sonraki adımları deneyin:



Bize ulaşın

Bize daha fazla bilgi verin, size yardımcı olalım