Programmrichtlinien für Entwickler

(gültig ab dem 31. August 2023, sofern nicht anders angegeben)

Gemeinsam zur weltweit vertrauenswürdigsten Quelle für Apps und Spiele werden

Ihre Ideen sind der Antrieb für unseren gemeinsamen Erfolg. Das bringt jedoch auch Verantwortung mit sich. Diese Programmrichtlinien für Entwickler sorgen zusammen mit der Vertriebsvereinbarung für Entwickler dafür, dass wir auch weiterhin über einer Milliarde Menschen die weltweit innovativsten und vertrauenswürdigsten Apps bei Google Play anbieten können. Unsere Richtlinien können Sie sich unten ansehen.

Inhaltsbeschränkungen

Nutzer aus aller Welt verwenden täglich Apps und Spiele von Google Play. Bevor Sie eine App einreichen, sollten Sie sich folgende Frage stellen: Ist meine App für Google Play angemessen und entspricht sie allen geltenden Gesetzen?

Gefährdung von Kindern

Apps, in denen es Nutzern nicht verboten wird, Inhalte zu erstellen, hochzuladen oder zu verbreiten, die die Ausbeutung oder den Missbrauch von Kindern unterstützen, werden umgehend aus Google Play entfernt. Hierzu zählen auch alle Darstellungen des sexuellen Missbrauchs von Kindern. Wenn Sie Inhalte in einem Google-Produkt melden möchten, durch die möglicherweise ein Kind ausgebeutet wird, klicken Sie auf **Missbrauch melden** . Sollten Sie an anderer Stelle im Internet auf entsprechende Inhalte stoßen, wenden Sie sich direkt an die entsprechende Behörde in Ihrem Land .

Die Nutzung von Apps, durch die Kinder gefährdet werden, ist nicht zulässig. Dazu gehört unter anderem die Nutzung von Apps, die sexuell missbräuchliches Verhalten gegenüber Kindern fördern, zum Beispiel:

- Unangemessene, auf ein Kind gerichtete Handlungen, z. B. Grapschen oder Streicheln
- Cyber-Grooming, z. B. Onlinefreundschaft mit einem Kind, um online oder offline sexuellen Kontakt herzustellen und/oder sexuelle Bilder mit diesem Kind auszutauschen
- Sexualisierung von Minderjährigen, z. B. Bilder, die den sexuellen Missbrauch von Kindern zeigen, propagieren oder dazu animieren oder Kinder auf eine Weise darstellen, die zur sexuellen Ausbeutung von Kindern führen könnte
- Sexuelle Erpressung, z. B. Bedrohung oder Erpressung eines Kindes durch echten oder vermeintlichen Zugriff auf intime Bilder dieses Kindes
- Kinderhandel, z. B. das Anbieten oder die Anwerbung von Kindern mit dem Ziel des kommerziellen sexuellen Missbrauchs

Wir ergreifen entsprechende Maßnahmen, wenn wir auf Inhalte mit Darstellungen des sexuellen Missbrauchs von Kindern aufmerksam werden, und senden beispielsweise einen Bericht an das Nationale Zentrum für vermisste und ausgebeutete Kinder (National Center for Missing & Exploited Children – NCMEC). Wenn Sie vermuten, dass ein Kind Opfer von Missbrauch, Ausbeutung oder Menschenhandel wurde oder entsprechend gefährdet ist, wenden Sie sich bitte umgehend an die örtliche Strafverfolgungsbehörde und an eine Kinderschutzorganisation aus dieser Liste .

Außerdem sind Apps verboten, die auf Kinder ausgerichtet sind, aber nicht jugendfreie Themen enthalten, einschließlich, aber nicht beschränkt auf:

- Apps mit übermäßiger Darstellung von Gewalt und Blutvergießen
- Apps, die schädliche und gefährliche Aktivitäten darstellen oder fördern

Apps, die ein negatives Körper- oder Selbstbild fördern, sind ebenfalls unzulässig. Dazu gehören unter anderem Apps, die zu Unterhaltungszwecken Schönheitsoperationen, Gewichtsabnahme und andere kosmetische Korrekturen des Aussehens einer Person darstellen.

Unangemessene Inhalte

Da Google Play eine sichere und respektvolle Plattform bleiben soll, haben wir Richtlinien entwickelt, in denen schädliche oder unangemessene Inhalte definiert und verboten werden.

Pornografische Inhalte und vulgäre Sprache

Apps, die pornografische Inhalte oder vulgäre Sprache enthalten oder dafür werben, einschließlich Inhalten und Diensten, die der sexuellen Befriedigung dienen, sind nicht zulässig. Darüber hinaus erlauben wir keine Apps oder App-Inhalte, die sexuelle Handlungen gegen Bezahlung bewerben oder dazu aufrufen. Wir erlauben keine Apps, die Inhalte mit sexuell missbräuchlichem Verhalten enthalten oder bewerben oder nicht einvernehmliche sexuelle Inhalte verbreiten. Nacktheit ist unter Umständen erlaubt, wenn sie hauptsächlich pädagogischen, dokumentarischen, wissenschaftlichen oder künstlerischen Zwecken dient und ihre Darstellung nicht grundlos ist.

Wenn eine App Inhalte enthält, die gegen diese Richtlinie verstoßen, aber in einer bestimmten Region als angemessen erachtet werden, kann die App Nutzern in dieser Region zur Verfügung gestellt werden, während sie für Nutzer in anderen Regionen nicht verfügbar ist.

Da Google Play eine sichere und respektvolle Plattform bleiben soll, haben wir Richtlinien entwickelt, in denen schädliche oder unangemessene Inhalte definiert und verboten werden.

- Darstellungen von Nacktheit sexueller Natur oder sexuell anzüglichen Posen, in denen eine Person gänzlich unbekleidet, weichgezeichnet oder nur minimal bekleidet ist und/oder die Art der Kleidung in einem öffentlichen Rahmen unangemessen wäre
- Darstellungen, Animationen oder Illustrationen sexueller Handlungen oder sexuell anzüglicher Posen oder die sexuelle Darstellung von Körperteilen
- Inhalte, die Sexspielzeug, Sexanleitungen, illegale sexuelle Themen und Fetische darstellen oder an sich als sexuelle Hilfsmittel dienen
- Anstößige oder vulgäre Inhalte, einschließlich, aber nicht beschränkt auf Obszönitäten, Beleidigungen, anstößige Texte oder nicht jugendfreie oder sexuelle Suchbegriffe im Store-Eintrag oder in der App
- Inhalte, die Sodomie darstellen, beschreiben oder dazu aufrufen
- Apps, in denen sexuelle Unterhaltung, Begleitservices oder andere Dienste beworben werden, die als Angebot sexueller Handlungen im Austausch gegen Bezahlung oder als Aufruf dazu angesehen werden können, einschließlich, aber nicht beschränkt auf Enjokōsai oder andere sexuelle Vereinbarungen, bei denen von einer der Parteien erwartet wird, dass sie der anderen Partei Geld, Geschenke oder finanzielle Unterstützung zukommen lässt („Sugardating“)
- Apps, die Personen entwürdigen oder vergegenständlichen, z. B. Apps, in denen behauptet wird, sie würden Personen entkleiden oder durch Kleidung hindurchsehen können, auch wenn die Apps als „Scherz“- oder Unterhaltungs-Apps gekennzeichnet sind
- Inhalte oder Verhaltensweisen, die darauf abzielen, Menschen auf sexuelle Weise zu bedrohen oder auszubeuten, wie z. B. Creepshots, versteckte Kameras, nicht einvernehmliche sexuelle Inhalte, die mit Deepfake- oder ähnlichen Technologien erstellt wurden, oder Inhalte, in denen es zu sexuellen Übergriffen kommt.

Hassrede/Volksverhetzung

Apps, in denen zu Gewalt oder Hass gegen Einzelpersonen oder Gruppen auf der Grundlage von ethnischer Herkunft, Religion, Behinderung, Alter, Nationalität, Veteranenstatus, sexueller Orientierung, Geschlecht, Geschlechtsidentität, Kaste, Einwanderungsstatus oder ähnlichen Eigenschaften aufgerufen wird, die mit systematischer Diskriminierung oder Ausgrenzung in Verbindung stehen, sind nicht zulässig.

Apps, die bildungsbezogene, dokumentarische, wissenschaftliche oder künstlerische Inhalte im Zusammenhang mit Nazis enthalten, können in bestimmten Ländern gemäß den dortigen Gesetzen und Vorschriften gesperrt werden.

Da Google Play eine sichere und respektvolle Plattform bleiben soll, haben wir Richtlinien entwickelt, in denen schädliche oder unangemessene Inhalte definiert und verboten werden.

- Inhalte oder Äußerungen, denen zufolge eine geschützte Gruppe unmenschlich, minderwertig oder hassenswert ist
- Apps, die hasserfüllte Verunglimpfungen, Stereotype oder Theorien enthalten, denen zufolge eine geschützte Gruppe negative Eigenschaften hat – z. B. niederträchtig, korrupt, böse usw. – oder die direkt oder indirekt behaupten, dass die Gruppe eine Bedrohung darstellt
- Inhalte oder Aussagen, mit denen andere Personen davon überzeugt werden sollen, dass bestimmte Menschen gehasst oder diskriminiert werden sollten, weil sie zu einer geschützten Gruppe gehören
- Inhalte, die für Materialien, Verhaltensweisen oder Symbole wie Flaggen und Abzeichen werben, die im Zusammenhang mit Hassgruppen stehen

Gewalt

Apps, die willkürliche Gewalt oder andere gefährliche Aktivitäten zeigen oder begünstigen, sind nicht zulässig. Apps, in denen fiktive Gewalt im Zusammenhang mit einem Spiel dargestellt wird, z. B. Zeichentrick, Jagd oder Angeln, sind generell zulässig.

Da Google Play eine sichere und respektvolle Plattform bleiben soll, haben wir Richtlinien entwickelt, in denen schädliche oder unangemessene Inhalte definiert und verboten werden.

- Grafische Darstellungen oder Beschreibungen von realistischer Gewalt oder Gewaltandrohungen gegenüber Personen oder Tieren
- Apps, die zu Selbstverletzung, Selbstmord, Essstörungen, Würgespielen oder anderen Aktivitäten, die gesundheitliche Folgen bis hin zum Tod haben können, anleiten

Terroristische Inhalte

Terroristische Organisationen dürfen für keinerlei Zwecke Apps bei Google Play veröffentlichen. Dies schließt die Rekrutierung ein.

Inhalte, die in Verbindung zu Terrorismus stehen, sind nicht zulässig. Dazu zählen Inhalte, in denen zu Terrorakten bzw. Gewalt aufgerufen wird oder Terroranschläge verherrlicht werden. Wenn Sie Inhalte, die sich auf jegliche Form von Terrorismus beziehen, im Kontext von Bildung, Dokumentation, Wissenschaft oder Kunst posten, sollten Sie darauf achten, genügend entsprechende Hintergrundinformationen zu liefern.

Gefährliche Organisationen und Bewegungen

Bewegungen oder Organisationen, die Gewalttaten gegen die Zivilbevölkerung verübt, vorbereitet oder dafür Verantwortung übernommen haben, ist es nicht erlaubt, Apps zu einem beliebigen Zweck, einschließlich der Rekrutierung, bei Google Play zu veröffentlichen.

Wir gestatten keine Apps mit Inhalten, in denen Gewalt gegen die Zivilbevölkerung geplant, vorbereitet oder verherrlicht wird. Wenn Ihre App solche Inhalte für einen pädagogischen, dokumentarischen, wissenschaftlichen oder künstlerischen Zweck enthält, muss gemeinsam mit diesen Inhalten auch der relevante Kontext angegeben werden.

Sensible Ereignisse

Apps, die aus sensiblen Ereignissen mit erheblichen sozialen, kulturellen oder politischen Auswirkungen wie Gefahren für die Bevölkerung, Naturkatastrophen, Krisenfällen im Bereich der öffentlichen Gesundheit, Konflikten, Todesfällen oder anderen tragischen Ereignissen einen Nutzen zu ziehen versuchen oder in solchen Fällen mangelnde Sensibilität zeigen, sind nicht zulässig. Apps mit Inhalten, die sich auf ein sensibles Ereignis beziehen, sind in der Regel zulässig, wenn diese Inhalte bildungsbezogenen, dokumentarischen, wissenschaftlichen oder künstlerischen Wert haben oder darauf abzielen, Nutzer zu warnen oder auf das sensible Ereignis aufmerksam zu machen.

Da Google Play eine sichere und respektvolle Plattform bleiben soll, haben wir Richtlinien entwickelt, in denen schädliche oder unangemessene Inhalte definiert und verboten werden.

- Mangelnde Sensibilität in Bezug auf den Tod einer echten Person oder Personengruppe durch Suizid, Überdosis, natürliche Todesursache usw.
- Leugnen eines gut dokumentierten, bedeutenden tragischen Ereignisses
- Profitieren von einem sensiblen Ereignis ohne erkennbaren Vorteil für die Opfer
- Apps, die gegen den Artikel zu Anforderungen für Apps im Zusammenhang mit dem Coronavirus bzw. der Krankheit COVID-19 verstoßen

Mobbing und Belästigung

Apps, die Drohungen, Belästigungen oder Mobbing enthalten oder begünstigen, sind nicht zulässig.

Da Google Play eine sichere und respektvolle Plattform bleiben soll, haben wir Richtlinien entwickelt, in denen schädliche oder unangemessene Inhalte definiert und verboten werden.

- Mobben von Opfern internationaler oder religiöser Konflikte
- Inhalte, durch die Dritte ausgebeutet werden, z. B. Erpressung, Chantage usw.
- Posten von Inhalten mit dem Ziel, Dritte öffentlich zu demütigen
- Belästigen von Opfern tragischer Vorfälle oder deren Freunden oder Angehörigen

Gefährliche Produkte

Wir gestatten keine Apps, die den Verkauf von Sprengstoffen, Schusswaffen, Munition oder bestimmtem Waffenzubehör ermöglichen.

- Eingeschränktes Zubehör umfasst Zubehör, mit dem mit Waffen automatische Schusswaffen simuliert oder Waffen in automatische Schusswaffen umgewandelt werden können, wie Bump Stocks, Gatling-Abzüge, Vollautomatik-Unterbrecher und Umbausätze, sowie Magazine oder Munitionsgurte mit über 30 Patronen.

Wir gestatten keine Apps mit Anleitungen für die Herstellung von Sprengstoffen, Schusswaffen, Munition, eingeschränktem Waffenzubehör oder anderen Waffen. Dies schließt Anleitungen zum Umbauen von Schusswaffen in automatische oder simulierte automatische Waffen ein.

Marihuana

Apps, die den Verkauf von Marihuana oder marihuanahaltigen Produkten ermöglichen, sind ungeachtet der jeweiligen Rechtslage nicht zulässig.

Da Google Play eine sichere und respektvolle Plattform bleiben soll, haben wir Richtlinien entwickelt, in denen schädliche oder unangemessene Inhalte definiert und verboten werden.

- Gestattung von Marihuanabestellungen über eine Einkaufswagen-Funktion innerhalb der App
- Unterstützung von Nutzern bei der Lieferung oder Abholung von Marihuana
- Ermöglichung des Verkaufs von Produkten, die THC (Tetrahydrocannabinol) enthalten, einschließlich Produkten wie THC-haltigen CBD-Ölen

Tabak und Alkohol

Wir gestatten keine Apps, die den Verkauf von Tabak, einschließlich E-Zigaretten und Vape Pens, ermöglichen oder den illegalen oder unangemessenen Konsum von Alkohol oder Tabak fördern.

Weitere Informationen

- Darstellungen des Konsums oder Verkaufs von Alkohol oder Tabak durch bzw. an Minderjährige oder entsprechende Aufrufe sind nicht gestattet.
- Es darf nicht der Eindruck erweckt werden, dass der Konsum von Tabak zu einem höheren Ansehen in sozialer, sexueller, beruflicher, intellektueller oder sportlicher Hinsicht verhilft.
- Die vorteilhafte Darstellung von übermäßigem Alkoholkonsum, einschließlich der positiven Darstellung von übermäßigem Alkoholkonsum, Trinkgelagen oder Trinkwettbewerben ist nicht gestattet.
- Die Bewerbung, Promotion oder auffällige Platzierung von Tabakprodukten (z. B. durch Werbung, Banner, Kategorien und Links zu Websites, auf denen Tabak verkauft wird) ist nicht gestattet.
- Der eingeschränkte Verkauf von Tabakprodukten in Apps für die Lieferung von Lebensmitteln kann in bestimmten Regionen zulässig sein, sofern eine Altersprüfung erfolgt und Sicherheitsvorkehrungen getroffen werden (z. B. durch Vorlage eines amtlichen Ausweises bei Lieferung).

Finanzdienstleistungen

Apps mit betrügerischen oder schädlichen Finanzprodukten und -dienstleistungen sind nicht zulässig.

Im Rahmen dieser Richtlinie sind unter Finanzprodukten und -dienstleistungen Produkte und Leistungen in Zusammenhang mit der Verwaltung oder Anlage von Geld und Kryptowährungen zu verstehen, einschließlich persönlicher Beratung.

Falls Ihre App Finanzprodukte und -dienstleistungen enthält oder bewirbt, müssen Sie die örtlichen und nationalen Bestimmungen für alle Regionen und Länder einhalten, auf die Ihre App ausgerichtet ist. So kann es gemäß der örtlichen Gesetzgebung beispielsweise erforderlich sein, bestimmte Informationen offenzulegen.

Entwickler von Apps mit Finanzfunktionen müssen das Erklärungsformular für Finanzfunktionen in der Play Console ausfüllen.

Binäre Optionen

Apps, in denen Nutzer mit binären Optionen handeln können, sind nicht zulässig.

Kryptowährungen

Wir gestatten keine Apps, die Kryptowährung auf Geräten minen. Apps, mit denen das Mining von Kryptowährung per Fernzugriff verwaltet werden kann, sind zulässig.

Privatkredite

Wir definieren einen Privatkredit als ein einmaliges Darlehen, das eine Einzelperson, ein Unternehmen oder ein Rechtssubjekt einer Privatperson gewährt. Mit einem Privatkredit darf außerdem weder der Kauf eines Anlagegegenstands noch eine Aus- oder Weiterbildung finanziert werden. Nutzer von Privatkrediten benötigen Informationen zu Qualität, Ausstattung, Gebühren, Kreditlaufzeit, Risiken und Vorteilen von Kreditprodukten, um fundierte Entscheidungen darüber treffen zu können, ob sie den Kredit aufnehmen.

- Beispiele: Privatkredite, Kurzzeitkredite, Peer-to-Peer-Kredite, Pfandkredite
- Nicht inbegriffen: Hypotheken, Autokredite, revolvierende Kreditlinien (z. B. Kreditkarten, persönliche Kreditlinien)

Für Apps, die Privatkredite anbieten, einschließlich, aber nicht beschränkt auf Apps, die Kredite direkt anbieten, Lead-Generatoren und Apps, die direkten Kontakt zwischen Kunden und als Kreditgeber fungierenden Dritten herstellen, muss in der Play Console die App-Kategorie „Finanzen“ festgelegt sein. Außerdem müssen die App-Metadaten folgende Informationen enthalten:

- Minimale und maximale Kreditlaufzeit
- Maximaler effektiver Jahreszins, zu dem in der Regel der Zinssatz zuzüglich Gebühren und anderer Kosten für ein Jahr zählt, oder ein ähnlicher anderer Satz, der gemäß geltenden gesetzlichen Vorschriften berechnet wird
- Ein typisches Beispiel für die Gesamtkosten des Kredits, einschließlich des Darlehensbetrags sowie aller anfallenden Gebühren
- Eine Datenschutzerklärung, in der der Zugriff auf sowie die Erhebung, Verwendung und Weitergabe von personenbezogenen und vertraulichen Nutzerdaten umfassend offengelegt wird

Wir lassen keine Apps zu, die Privatkredite bewerben, deren vollständige Rückzahlung innerhalb von 60 Tagen oder weniger ab dem Datum der Kreditgewährung erfolgen muss. Solche Kredite bezeichnen wir als kurzfristige Privatkredite.

Wir müssen in der Lage sein, eine Verbindung zwischen Ihrem Entwicklerkonto und allen zur Verfügung gestellten Lizenzen und Dokumenten herzustellen, die nachweisen, dass Sie Privatkredite anbieten können. Wir bitten Sie möglicherweise um zusätzliche Informationen oder Dokumente, um zu bestätigen, dass Ihr Konto alle lokalen Gesetze und Bestimmungen einhält.

Privatkredit-Apps oder Apps, deren Hauptzweck der Zugriff auf Privatkredite (z. B. Lead-Generatoren oder Vermittlung) ist, dürfen nicht auf sensible Daten wie Fotos und Kontakte zugreifen. Die folgenden Berechtigungen sind unzulässig:

- Read_external_storage
- Read_media_images
- Read_contacts
- Access_fine_location
- Read_phone_numbers
- Read_media_videos

Privatkredite mit hohem effektivem Jahreszins

In den Vereinigten Staaten lassen wir keine Apps für Privatkredite zu, bei denen der effektive Jahreszins bei 36% oder höher liegt. Für Apps, in denen Privatkredite in den Vereinigten Staaten angeboten werden, muss der maximale effektive Jahreszins angegeben werden. Dieser ist entsprechend der Vorgaben des Truth in Lending Act (TILA) zu berechnen.

Diese Richtlinien gelten für Apps, in denen Kredite direkt angeboten werden, für Lead-Generatoren und für Apps, durch die direkter Kontakt zwischen Kunden und als Kreditgeber fungierenden Dritten hergestellt wird.

Länderspezifische Anforderungen

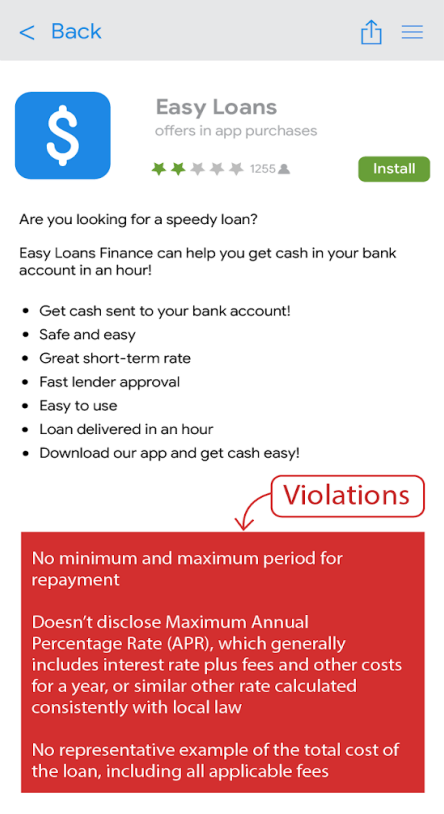
Im Rahmen der Erklärung zu Finanzfunktionen in der Play Console müssen für Privatkredit-Apps, die auf die aufgeführten Länder ausgerichtet sind, zusätzliche Anforderungen erfüllt und zusätzliche Unterlagen zur Verfügung gestellt werden. Auf Anfrage von Google Play müssen Sie zusätzliche Informationen oder Unterlagen zur Verfügung stellen, aus denen Ihre Einhaltung der behördlichen Vorschriften und Lizenzanforderungen hervorgeht.

1. **Indien**
   - Wenn Sie Privatkredite auf der Grundlage einer Lizenz der Reserve Bank of India (RBI) anbieten, müssen Sie uns eine Kopie dieser Lizenz zur Überprüfung einreichen.
   - Wenn Sie nicht direkt Kredite anbieten, sondern lediglich eine Plattform, über die sich Nutzer Geld bei registrierten Nichtbanken (Non-Banking Finance Company, NBFCs) oder Banken leihen

können, müssen Sie dies in der Erklärung genau angeben.
    - Außerdem müssen die Namen aller registrierten NBFCs oder Banken in der Beschreibung Ihrer App deutlich offengelegt werden.
2. **Indonesien**
    - Wenn mit Ihrer App IT-gestützte Kreditdienste gemäß der OJK-Verordnung Nr. 77/POJK.01/2016 (in der jeweils gültigen Fassung) angeboten werden, müssen Sie uns eine Kopie Ihrer gültigen Lizenz zur Überprüfung vorlegen.
3. **Philippinen**
    - Alle Finanz- und Kreditunternehmen, die Kredite über entsprechende Onlineplattformen anbieten, müssen bei der philippinischen Securities and Exchange Commission (SEC) eine SEC-Registrierungs- und eine Zulassungsnummer (CA-Nummer, Certificate of Authority) beantragen.
        - Außerdem müssen Sie in der Beschreibung Ihrer App den Namen Ihres Unternehmens sowie seinen offiziellen Namen, die SEC-Registrierungsnummer und die Zulassung zum Betrieb (Certificate of Authority) eines Finanz-/Kreditunternehmens angeben.
    - Apps, die der Kreditvergabe über Crowdfundingaktivitäten dienen, wie Peer-to-Peer-Kredite (P2P-Kredite), oder den CF-Regeln (Rules and Regulations Governing Crowdfunding, zu Deutsch: Regeln und Vorschriften für Crowdfunding) des SEC unterliegen, müssen Transaktionen über SEC-registrierte CF-Vermittler abwickeln.
4. **Nigeria**
    - Digitale Geldverleiher (Digital Money Lenders, DML) müssen sich an die jeweils gültige Fassung der LIMITED INTERIM REGULATORY/REGISTRATION FRAMEWORK AND GUIDELINES FOR DIGITAL LENDING, 2022 (BESCHRÄNKTER VORLÄUFIGER RECHTS-/REGISTRIERUNGSRAHMEN SOWIE RICHTLINIEN FÜR DEN DIGITALEN VERLEIH 2022) von der FCCPC (Federal Competition and Consumer Protection Commission, zu Deutsch: Bundeskommission für den Schutz von Wettbewerb und Verbrauchern) von Nigeria halten und ein überprüfbares Genehmigungsschreiben von der FCCPC erlangen.
    - Kreditaggregatoren müssen Unterlagen und/oder eine Zertifizierung für digitale Kreditdienste sowie die Kontaktdaten jedes DML-Partners zur Verfügung stellen.
5. **Kenia**
    - Digitale Kreditinstitute (Digital Credit Providers, DCPs) müssen die DCP-Registrierung durchlaufen und eine Lizenz von der Central Bank of Kenya (CBK) erlangen. Im Rahmen Ihrer Erklärung müssen Sie eine Kopie Ihrer Lizenz von der CBK zur Verfügung stellen.
    - Wenn Sie nicht direkt Kredite anbieten, sondern lediglich eine Plattform, über die sich Nutzer Geld bei registrierten DCPs leihen können, müssen Sie dies in der Erklärung genau angeben und eine Kopie der DCP-Lizenz von Ihren jeweiligen Partnern beifügen.
    - Momentan akzeptieren wir Erklärungen und Lizenzen nur von Rechtssubjekten, die im Directory of Digital Credit Providers (Verzeichnis digitaler Kreditinstitute) auf der offiziellen Website der CBK aufgeführt sind.
6. **Pakistan**
    - Jedes Finanzunternehmen, das Kredite anbietet und keine Bank ist, (Non-Banking Finance Company, NBFC) darf nur eine digitale Kredit-App (Digital Lending App, DLA) anbieten. Falls Sie mehr als eine Kredit-App pro Finanzunternehmen veröffentlichen, können Ihr Entwicklerkonto und alle damit verknüpften Konten geschlossen werden.
    - Sie müssen einen von der SECP bestätigten Nachweis erbringen, um in Pakistan digitale Kreditdienstleistungen anbieten zu können.
7. **Thailand**
    - Für Privatkredit-Apps, die auf Thailand ausgerichtet sind, ist eine gültige Lizenz der Bank of Thailand (BoT) erforderlich. Entwickler müssen entsprechende Unterlagen einreichen, um nachzuweisen, dass sie Privatkredite anbieten oder die Gewährung eines Privatkredits in Thailand erleichtern können, darunter:

- Eine Kopie der von der Bank of Thailand ausgestellten Lizenz für die Tätigkeit als Anbieter von Privatkrediten oder Nano-Finance-Unternehmen.

Da Google Play eine sichere und respektvolle Plattform bleiben soll, haben wir Richtlinien entwickelt, in denen schädliche oder unangemessene Inhalte definiert und verboten werden.



Glücksspiele, Spiele und Wettbewerbe, bei denen um echtes Geld gespielt wird

Apps für Glücksspiele um echtes Geld, Anzeigen für Glücksspiele um echtes Geld, gamifizierte Treuepunkteprogramme und Daily-Fantasy-Sports-Apps sind zulässig, solange sie bestimmte Anforderungen erfüllen.

Glücksspiel-Apps

Vorbehaltlich der Einschränkungen und der Konformität mit allen Google Play-Richtlinien sind Apps, die Online-Glücksspiele in ausgewählten Ländern ermöglichen oder erleichtern, zulässig, sofern der Entwickler das Antragsverfahren für bei Google Play veröffentlichte Glücksspiel-Apps erfolgreich durchläuft, ein staatlicher Betreiber ist und/oder als lizenzierter Betreiber bei der zuständigen Behörde für Glücksspiel im jeweiligen Land gemeldet ist und in diesem Land über eine gültige Betriebserlaubnis für die Art des Online-Glücksspielprodukts verfügt, die er anbieten möchte.

Wir genehmigen nur seriöse lizenzierte oder autorisierte Glücksspiel-Apps, über die die folgenden Arten von Online-Glücksspielprodukten angeboten werden:

- Online-Casinospiele
- Sportwetten
- Pferderennen (sofern diese getrennt von Sportwetten reguliert und lizenziert sind)
- Lotterien
- Daily Fantasy Sports

Infrage kommende Apps müssen folgende Anforderungen erfüllen:

- Der Entwickler muss das Antragsverfahren durchlaufen, um die App bei Google Play anbieten zu können.
- Die App muss alle geltenden Gesetze und Branchenstandards für jedes Land erfüllen, in dem sie angeboten wird.
- Der Entwickler muss eine gültige Glücksspiellizenz für jedes Land oder jeden Bundesstaat / jedes Territorium haben, in dem die App angeboten wird.
- Der Entwickler darf keine Art von Glücksspielprodukt anbieten, die von seiner Glücksspiellizenz nicht abgedeckt wird.
- Die App muss so konzipiert sein bzw. über entsprechende Mechanismen verfügen, dass Minderjährige sie nicht nutzen können.
- In Ländern, Bundesstaaten/Territorien oder Regionen, für die der Entwickler keine Glücksspiellizenz besitzt, muss der Zugriff auf die App und ihre Nutzung verhindert werden.
- Die App darf NICHT als kostenpflichtige App bei Google Play angeboten werden und für die App darf nicht die Google Play In-App-Abrechnung genutzt werden.
- Die App muss kostenlos aus dem Google Play Store herunterladbar und installierbar sein.
- Die App muss als AO (Adult Only, z. Dt. „nur für Erwachsene geeignet“) oder durch ein äquivalentes Alterskennzeichen nach dem IARC-System gekennzeichnet sein.
- Die App und der dazugehörige App-Eintrag müssen gut sichtbare Informationen zu verantwortungsbewusstem Glücksspiel enthalten.

Andere Apps für Spiele, Wettbewerbe und Turniere um echtes Geld

Für alle anderen Apps, die die oben genannten Teilnahmevoraussetzungen für Glücksspiel-Apps nicht erfüllen und die nicht in den unten genannten „anderen Pilotprojekten für Spiele, bei denen um echtes Geld gespielt wird“ enthalten sind, sind Inhalte oder Dienste unzulässig, die es Nutzern ermöglichen oder erleichtern, echtes Geld für Wetten, Einsätze oder Teilnahme (einschließlich mit Geld gekaufter In-App-Artikel) zu verwenden, um einen Preis von echtem Geldwert zu erhalten. Dazu gehören unter anderem Onlinecasinos, Sportwetten, Lotterien und Spiele, bei denen Geld angenommen und Geld- oder Sachpreise ausgeschrieben werden (Ausnahme: Programme, die gemäß den unten beschriebenen Anforderungen für gamifizierte Treuepunkteprogramme zugelassen sind).

Beispiele für Verstöße

- Spiele, bei denen für Geld um Sach- oder Geldpreise gespielt werden kann
- Apps mit Navigationselementen oder -funktionen (Menüpunkte, Tabs, Schaltflächen, WebViews usw.), die einen Call-to-Action zum Wetten oder Teilnehmen an Spielen, Wettbewerben oder Turnieren mit echtem Geld enthalten, z. B. Apps, die Nutzer dazu auffordern, auf „WETTEN!“, „ANMELDEN!“ oder „TEILNEHMEN!“ zu tippen, um einen Geldpreis zu gewinnen
- Apps, die Wetteinsätze, In-App-Währungen, Gewinne oder Einzahlungen annehmen oder verwalten, durch die der Nutzer die Möglichkeit erhält, um Geld- oder Sachpreise zu spielen oder diese zu gewinnen

Pilottests für „Andere Apps für Spiele, Wettbewerbe und Turniere um echtes Geld“

In ausgewählten Regionen führen wir möglicherweise gelegentlich zeitlich begrenzte Pilotprojekte für bestimmte Typen von Apps durch, in denen um echtes Geld gespielt wird. Weitere Informationen diesbezüglich erhalten Sie auf dieser Hilfeseite. Das Pilotprojekt zu Online-Greifautomaten-Spielen in Japan endete am 11. Juli 2023. Ab dem 12. Juli 2023 können Apps mit Online-Greifautomaten-Spielen weltweit bei Google Play aufgeführt werden, wenn sie geltende Gesetze einhalten und bestimmte Anforderungen erfüllen.

Gamifizierte Treuepunkteprogramme

Wenn gesetzlich zulässig und nicht durch zusätzliche Lizenzvorgaben für Glücksspiele oder Spiele eingeschränkt, genehmigen wir Treuepunkteprogramme, bei denen Nutzer Prämien (Sachpreise oder

gleichwertige Geldbeträge) erhalten können, sofern sie die folgenden Play Store-Teilnahmevoraussetzungen erfüllen:

Für alle Apps (Spiele und Apps, die keine Spiele sind):

- Bei Vorteilen, Prämien oder Belohnungen, die im Rahmen des Treuepunkteprogramms gewährt werden, muss klar und deutlich erkennbar sein, dass diese im Hinblick auf anrechnungsfähige monetäre Transaktionen in der App als ergänzend und untergeordnet anzusehen sind. Die anrechnungsfähige monetäre Transaktion muss eine echte separate Transaktion für Güter oder Dienstleistungen sein, die unabhängig vom Treuepunkteprogramm ist. Außerdem dürfen diese Vorteile, Prämien und Belohnungen nicht gekauft oder durch beliebige andere Arten des Austauschs erworben werden, die anderweitig gegen die Einschränkungen in der Richtlinie zu Glücksspielen, Spielen und Wettbewerben, bei denen um echtes Geld gespielt wird, verstoßen.
  - So darf kein Teil der anrechnungsfähigen monetären Transaktion eine Gebühr oder einen Wetteinsatz für die Teilnahme am Treuepunkteprogramm darstellen. Außerdem darf sie nicht zum Kauf von Gütern oder Dienstleistungen über dem regulären Preis führen.

Für Spiele :

- Treuepunkte oder Prämien mit Vorteilen, Vergünstigungen oder Belohnungen, die in Verbindung mit einer anrechnungsfähigen monetären Transaktion stehen, dürfen nur auf Grundlage eines festgelegten Verhältnisses vergeben und eingelöst werden, wobei das Verhältnis in der App und auch in den öffentlich verfügbaren offiziellen Regeln für das Programm detailliert dokumentiert sein muss. Die Vergabe von Vorteilen oder der Einlösungswert darf **nicht** auf Wett-, Prämien- oder Potenzierungsmechanismen basieren, die an die Leistung im Spiel gekoppelt sind oder auf Zufall beruhen.

Für Apps, die keine Spiele sind:

- Treuepunkte oder Prämien dürfen an einen Wettbewerb oder an Zufallsmechanismen gekoppelt werden, wenn sie die unten aufgeführten Voraussetzungen erfüllen. Für Treuepunkteprogramme, bei denen in Verbindung mit anrechnungsfähigen monetären Transaktionen Vorteile, Vergünstigungen oder Belohnungen vergeben werden, gelten folgende Voraussetzungen:
  - Die offiziellen Regeln für das Programm müssen innerhalb der App veröffentlicht werden.
  - Für Programme mit variablenbasierten, zufallsbasierten oder randomisierten Prämiensystemen: Nennen Sie in den offiziellen Bedingungen 1) für Prämienprogramme, die fixe Wahrscheinlichkeiten zur Bestimmung der Prämien verwenden, die Wahrscheinlichkeiten und 2) für alle anderen derartigen Programme die Auswahlmethode, z. B. die Variablen, die zur Bestimmung der Prämie verwendet werden.
  - Geben Sie in den offiziellen Bedingungen eines Programms, bei denen Ziehungen, Gewinnspiele oder ähnliche Mechanismen zum Einsatz kommen, je Aktion eine feste Anzahl von Gewinnern, eine feste Frist für die Einreichung und ein Datum für die Vergabe des Preises an.
  - Führen Sie ein etwaiges festes Verhältnis für das Sammeln und Einlösen von Treuepunkten oder Treueprämien deutlich sichtbar in der App ebenso wie in den offiziellen Bedingungen des Programms auf.

Art der App mit Treuepunkteprogramm	Gamifizierte Treueprogramme und variable Prämien	Treueprämien auf Grundlage eines festen Verhältnisses / festen Plans	Nutzungsbedingungen für das Treuepunkteprogramm	In den Nutzungsbedir müssen die Wahrscheinlich oder die Auswahlmetho alle Treuepunktepr mit Zufallsmechan offengelegt we
Spiel	Nicht zulässig	Zulässig	Erforderlich	Nicht zutreffend Spiele sind keine Zufallsmechanis Treuepunktepro zulässig)
App, die kein Spiel ist	Zulässig	Zulässig	Erforderlich	Erforderlich

Werbeanzeigen für Glücksspiele oder Spiele, Wettbewerbe und Turniere in bei Play angebotenen Apps, bei denen es um echtes Geld geht

Apps, in denen über Anzeigen für Glücksspiele oder Spiele, Wettbewerbe und Turniere, bei denen um echtes Geld gespielt wird, geworben wird, sind zulässig, sofern sie folgende Anforderungen erfüllen:

- App, Anzeige und auch der Werbetreibende selbst müssen alle geltenden Gesetze und Branchenstandards für jeden Standort erfüllen, an dem die Anzeige sichtbar ist.
- Die Anzeige muss alle geltenden Werbelizenzierungsanforderungen für alle beworbenen glücksspielbezogenen Produkte und Dienste erfüllen.
- In der App dürfen Personen, von denen der App-Anbieter weiß, dass sie jünger als 18 Jahre sind, keine Anzeigen für Glücksspiele gezeigt werden.
- Die App darf nicht am Designed for Families-Programm teilnehmen.
- Die App darf nicht auf Personen, die jünger als 18 Jahre sind, ausgerichtet sein.
- Bei Werbung für eine Glücksspiel-App (wie oben definiert) muss die Anzeige auf der Landingpage, im beworbenen App-Eintrag selbst oder in der App deutlich über verantwortungsbewusstes Glücksspiel informieren.
- Die App darf keine simulierten Glücksspielinhalte enthalten (z. B. Apps für soziale Casinospiele oder Apps mit virtuellen Spielautomaten).
- Die App darf keine Supportfunktionen für Glücksspiele oder Spiele, Lotterien und Turniere, bei denen um echtes Geld gespielt wird, bieten, z. B. Funktionen, die bei der Durchführung von Wetten, bei Auszahlungen, bei der Verfolgung von Gewinnen und Verlusten / Sportergebnissen / Wettquoten oder bei der Verwaltung der Teilnahmegebühren helfen.
- App-Inhalte dürfen nicht für Glücksspieldienste oder Dienste für Spiele, Lotterien oder Turniere, bei denen um echtes Geld gespielt wird, werben oder Nutzer dorthin weiterleiten.

Nur Apps, die alle oben aufgeführten Anforderungen erfüllen, dürfen Anzeigen für Glücksspiele oder Spiele, Lotterien oder Turniere, bei denen um echtes Geld gespielt wird, enthalten. Zugelassene Glücksspiel-Apps (wie oben definiert) oder zugelassene Daily-Fantasy-Sports-Apps (siehe unten), die die Anforderungen 1 bis 6 oben erfüllen, dürfen ebenso Anzeigen für Glücksspiele oder Spiele, Lotterien oder Turniere, bei denen um echtes Geld gespielt wird, enthalten.

Beispiele für Verstöße

- Eine App für Minderjährige mit Werbung für Glücksspieldienste
- Ein simuliertes Casinospiel, das für Casinos mit echtem Geld wirbt oder Nutzer dorthin weiterleitet

- Eine spezielle App zur Verfolgung von Sportwettquoten mit integrierten Glücksspiel-Werbeanzeigen, die auf eine Sportwetten-Website verweisen
- Apps mit Glücksspielanzeigen, die gegen unsere Richtlinie zu irreführender Werbung verstoßen, z. B. Anzeigen, die Nutzern als Schaltflächen, Symbole oder andere interaktive In-App-Elemente angezeigt werden

Daily Fantasy Sports-Apps (DFS)

Daily Fantasy Sports-Apps (DFS) gemäß den geltenden lokalen Gesetzen sind nur zulässig, wenn sie die folgenden Anforderungen erfüllen:

- 1) Die App ist nur in den Vereinigten Staaten erhältlich oder 2) sie erfüllt die oben genannten Anforderungen an Glücksspiel-Apps für Länder, bei denen es sich nicht um die Vereinigten Staaten handelt, und hat das oben genannte Antragsverfahren für diese Länder durchlaufen.
- Der Entwickler muss das DFS-Registrierungsverfahren durchlaufen und akzeptiert werden, um die App bei Google Play anbieten zu können.
- Die App muss allen geltenden Gesetzen und Branchenstandards für die Länder entsprechen, in denen sie vertrieben wird.
- Minderjährige Nutzer müssen durch die App daran gehindert werden, zu wetten oder Zahlungen vorzunehmen.
- Die App darf NICHT als kostenpflichtige App bei Google Play angeboten werden und die Google Play In-App-Abrechnung nicht nutzen.
- Die App muss kostenlos aus dem Play Store herunterladbar und installierbar sein.
- Die App muss als AO (Adult Only, z. Dt. „nur für Erwachsene geeignet“) oder durch ein äquivalentes Alterskennzeichen nach dem IARC-System gekennzeichnet sein.
- Die App und der dazugehörige App-Eintrag müssen gut sichtbare Informationen zu verantwortungsbewusstem Glücksspiel enthalten.
- Die App muss alle geltenden Gesetze und Branchenstandards für alle US-Bundesstaaten und -Territorien erfüllen, in denen sie angeboten wird.
- Der Entwickler muss eine gültige Glücksspiellizenz für alle US-Bundesstaaten und -Territorien haben, in denen eine Lizenz für Daily Fantasy Sports-Apps erforderlich ist.
- In US-Bundesstaaten und -Territorien, für die der Entwickler keine Lizenz für Daily Fantasy Sports-Apps besitzt, muss die Nutzung der App verhindert werden.
- In US-Bundesstaaten und -Territorien, in denen Daily Fantasy Sports-Apps nicht legal sind, muss die Nutzung der App verhindert werden.

Illegale Handlungen

Apps, die Raum für illegale Handlungen geben oder solche Handlungen unterstützen, sind nicht zulässig.

Da Google Play eine sichere und respektvolle Plattform bleiben soll, haben wir Richtlinien entwickelt, in denen schädliche oder unangemessene Inhalte definiert und verboten werden.

- Möglichkeit des Kaufs oder Verkaufs von illegalen Drogen
- Darstellung des Konsums oder Verkaufs von Drogen, Alkohol oder Tabak durch bzw. an Minderjährige oder Aufruf dazu
- Anleitung zum Anbau oder zur Herstellung illegaler Drogen

Von Nutzern erstellte Inhalte

Von Nutzern erstellte Inhalte sind Inhalte, die Nutzer zu einer App beitragen und die für mindestens einen Teil der anderen Nutzer der App sichtbar sind.

Apps, die von Nutzern erstellte Inhalte enthalten oder darauf verweisen, darunter Apps, die spezialisierte Browser oder Clients sind, über die Nutzer auf entsprechende Plattformen weitergeleitet werden, müssen zuverlässige, wirksame und dauerhafte Verfahren zur Moderation der von Nutzern erstellten Inhalte implementieren:

- Nutzer müssen die Nutzungsbedingungen und/oder Nutzerrichtlinien der App akzeptieren, bevor sie Inhalte erstellen oder hochladen dürfen.
- Unangemessene Inhalte und unangemessenes Verhalten müssen gemäß den Programmrichtlinien für Entwickler von Google Play definiert und in den Nutzungsbedingungen oder Nutzerrichtlinien der App untersagt werden.
- Es müssen angemessene, dauerhafte Verfahren zur Moderation der von Nutzern erstellten Inhalte implementiert werden, die den in der App gehosteten Inhalten gerecht werden.
  - Bei Augmented Reality-Apps (AR) müssen bei der Moderation der von Nutzern erstellten Inhalte (einschließlich des In-App-Berichtssystems) sowohl unangemessene von Nutzern erstellte AR-Inhalte (z. B. ein sexuell explizites AR-Bild) als auch sensible AR-Verankerungsorte (z. B. AR-Inhalte, die mit einem eingeschränkt zugänglichen Bereich wie einem Militärstützpunkt oder einem privaten Grundstück verankert sind, bei dem die AR-Verankerung Probleme für den Grundstückseigentümer verursachen kann) berücksichtigt werden.
- Die App muss ein System zum Melden unangemessener von Nutzern erstellter Inhalte umfassen und es müssen gegebenenfalls entsprechende Maßnahmen ergriffen werden.
- Die App muss ein System umfassen, mit dem von Nutzern erstellte Inhalte und Nutzer selbst blockiert werden können.
- Es müssen Absicherungen implementiert werden, um zu vermeiden, dass unangemessenes Nutzerverhalten durch In-App-Monetarisierung gefördert wird.

Nebensächliche pornografische Inhalte

Pornografische Inhalte gelten als „nebensächlich“, wenn sie in einer App mit von Nutzern erstellten Inhalten erscheinen, die (1) Zugriff auf hauptsächlich nicht pornografische Inhalte bietet und (2) nicht aktiv pornografische Inhalte bewirbt oder darauf verweist. Pornografische Inhalte, die nach anwendbarem Recht illegal sind, und Inhalte, die Kinder gefährden , werden nicht als „nebensächlich“ eingestuft und sind nicht zulässig.

Apps mit von Nutzern erstellten Inhalten dürfen nebensächliche pornografische Inhalte enthalten, sofern alle der folgenden Voraussetzungen erfüllt sind:

- Die betreffenden Inhalte sind standardmäßig hinter Filtern verborgen, bei denen mindestens zwei Nutzeraktionen erforderlich sind, um sie vollständig zu deaktivieren. Das kann z. B. ein Interstitial zur Verschleierung sein oder sie werden standardmäßig nicht angezeigt, es sei denn, die Funktion „SafeSearch“ ist deaktiviert.
- Kindern, wie in der Richtlinie für familienfreundliche Inhalte definiert, ist es ausdrücklich untersagt, auf Ihre App zuzugreifen. Dazu werden Systeme zur Altersüberprüfung eingesetzt, wie z. B. eine neutrale Altersabfrage oder ein nach anwendbarem Recht definiertes angemessenes System.
- Wie in der Richtlinie „Altersfreigaben“ vorgeschrieben, haben Sie für Ihre App die Fragen zu von Nutzern erstellten Inhalten im Fragebogen zur Altersfreigabe ordnungsgemäß beantwortet.

Apps, die in erster Linie unangemessene von Nutzern erstellte Inhalte enthalten, werden von Google Play entfernt. Das Gleiche gilt für Apps, die primär zum Hosten dieser Inhalte verwendet werden oder bei Nutzern einen entsprechenden Ruf erlangen.

Da Google Play eine sichere und respektvolle Plattform bleiben soll, haben wir Richtlinien entwickelt, in denen schädliche oder unangemessene Inhalte definiert und verboten werden.

- Werbung für von Nutzern erstellte, sexuell explizite Inhalte, einschließlich der Implementierung oder Zulassung kostenpflichtiger Funktionen, durch die die Verbreitung unangemessener Inhalte gefördert wird

- Apps mit von Nutzern erstellten Inhalten, denen ausreichende Sicherheitsvorkehrungen zum Schutz vor Drohungen, Belästigungen oder Mobbing fehlen, besonders im Hinblick auf Minderjährige
- Beiträge, Kommentare oder Fotos in einer App, mit denen in erster Linie eine andere Person belästigt oder herausgegriffen werden soll, ob aus Heimtücke oder um diese zu beschimpfen oder zu verhöhnen
- Apps, die Beschwerden von Nutzern zu unangemessenen Inhalten wiederholt nicht angehen

---

Gesundheitsbezogene Inhalte und Dienstleistungen

Apps mit Inhalten und Dienstleistungen, die der Gesundheit von Nutzern schaden, sind nicht zulässig.

Wenn Ihre App gesundheitsbezogene Inhalte und Dienstleistungen enthält oder bewirbt, muss sie allen geltenden Gesetzen und Bestimmungen entsprechen.

Verschreibungspflichtige Arzneimittel

Apps, die den Kauf oder Verkauf von verschreibungspflichtigen Medikamenten ohne Rezept ermöglichen, sind nicht zulässig.

Nicht freigegebene Substanzen

Google Play gestattet keine Apps, in denen nicht freigegebene Substanzen beworben oder verkauft werden. Jeglicher Anspruch auf Legalität wird dabei nicht berücksichtigt.

Da Google Play eine sichere und respektvolle Plattform bleiben soll, haben wir Richtlinien entwickelt, in denen schädliche oder unangemessene Inhalte definiert und verboten werden.

- Sämtliche Produkte in dieser nicht vollständigen Liste nicht freigegebener Arznei- und Nahrungsergänzungsmittel
- Produkte, die Ephedra enthalten
- Produkte, die humanes Choriongonadotropin (hCG) enthalten, wenn diese in Verbindung mit Gewichtsabnahme bzw. Gewichtskontrolle oder in Verbindung mit anabolen Steroiden beworben werden
- Pflanzliche und diätetische Nahrungsergänzungsmittel mit pharmazeutischen oder gesundheitsgefährdenden Wirkstoffen
- Falsche oder irreführende gesundheitsbezogene Angaben, beispielsweise wenn die Behauptung aufgestellt wird, diese Produkte seien so wirksam wie verschreibungspflichtige Arzneimittel oder Betäubungsmittel
- Behördlich nicht zugelassene Produkte, die so vermarktet werden, als seien sie sicher und könnten Krankheiten bzw. Beschwerden wirksam verhindern, heilen oder behandeln
- Produkte, für die staatliche oder behördliche Maßnahmen ergriffen wurden oder für die von staatlicher oder behördlicher Seite aus eine Warnung ausgegeben wurde
- Produkte mit Bezeichnungen, bei denen die Gefahr einer Verwechslung mit nicht freigegebenen Arznei- oder Nahrungsergänzungsmitteln bzw. mit Betäubungsmitteln besteht

Weitere Informationen zu den von uns überwachten nicht freigegebenen oder irreführenden Arznei- und Nahrungsergänzungsmitteln erhalten Sie unter www.legitscript.com .

Gesundheitsbezogene Fehlinformationen

Apps, die irreführende gesundheitsbezogene Behauptungen enthalten, die dem bestehenden medizinischen Konsens widersprechen oder Nutzern schaden können, sind nicht zulässig.

Da Google Play eine sichere und respektvolle Plattform bleiben soll, haben wir Richtlinien entwickelt, in denen schädliche oder unangemessene Inhalte definiert und verboten werden.

- Irreführende Behauptungen über Impfstoffe, z. B. dass Impfstoffe die DNA eines Menschen verändern können
- Befürworten von gefährlichen, nicht zugelassenen Behandlungen
- Befürworten anderer schädlicher gesundheitsbezogener Praktiken, z. B. Konversionstherapie

Anforderungen in Zusammenhang mit COVID-19

Apps müssen den Anforderungen an Apps im Zusammenhang mit dem Coronavirus bzw. der Krankheit COVID-19 entsprechen.

Medizinische Funktionen

Apps mit medizinischen oder gesundheitsbezogenen Funktionen, die irreführend oder potenziell schädlich sind, sind nicht zulässig. Dies gilt beispielsweise für Apps, die angeblich über Oximetriefunktionen verfügen, die aber rein App-basiert sind. Oximetrie-Apps müssen durch externe Hardware, Wearables oder spezifische Smartphone-Sensoren gestützt werden, die Oximetriefunktionen explizit unterstützen. Die Metadaten der unterstützten Apps müssen außerdem einen Haftungsausschluss enthalten, aus dem hervorgeht, dass die jeweilige App nicht für medizinische, sondern nur für allgemeine Fitness- und Wellnesszwecke bestimmt ist, und dass es sich nicht um ein Medizinprodukt handelt. Darüber hinaus muss das kompatible Hardware- bzw. Gerätemodell ordnungsgemäß angegeben werden.

Zahlungen — klinische Dienstleistungen

Für die Bezahlung regulierter klinischer Dienstleistungen darf das Abrechnungssystem von Google Play nicht verwendet werden. Weitere Informationen finden Sie im Hilfe-Artikel Die Zahlungsrichtlinie von Google Play .

Health Connect-Daten

Daten, auf die unter Verwendung von Berechtigungen für Health Connect zugegriffen wird, werden als personenbezogene und vertrauliche Nutzerdaten erachtet, die der Richtlinie zu Nutzerdaten und zusätzlichen Anforderungen unterliegen.

Geistiges Eigentum

Apps oder Entwicklerkonten, die die gewerblichen Schutzrechte Dritter verletzen, darunter Patent- und Markenrechte, Geschäftsgeheimnisse, Urheberrechte und andere Eigentumsrechte, sind nicht zulässig. Das gilt auch für Apps, die eine Verletzung gewerblicher Schutzrechte Dritter gutheißen oder dazu verleiten.

Wir gehen eindeutigen Hinweisen auf mutmaßliche Urheberrechtsverletzungen nach. In unseren Bestimmungen zum Urheberrecht finden Sie weitere Informationen zu diesem Thema. Dort können Sie auch einen DMCA-Antrag stellen.

Wenn Sie eine Beschwerde bezüglich des Verkaufs oder der Werbung für Produktfälschungen in einer App einreichen möchten, senden Sie uns bitte eine Mitteilung über Produktfälschungen .

Falls Sie als Markeninhaber glauben, dass eine App bei Google Play Ihre Markenrechte verletzt, empfehlen wir Ihnen, sich direkt mit dem Entwickler in Verbindung zu setzen, um die Angelegenheit zu klären. Kommt es zu keiner Einigung mit dem Entwickler, reichen Sie über dieses Formular eine Markenbeschwerde ein.

Wenn Sie einen schriftlichen Nachweis haben, dass Sie berechtigt sind, das geistige Eigentum eines Dritten, wie zum Beispiel Markennamen, Logos und Grafikinhalte, in Ihrer App oder Ihrem Store-Eintrag zu verwenden, kontaktieren Sie das Google Play-Team , bevor Sie Ihre App einreichen. So können Sie vermeiden, dass Ihre App aufgrund einer Verletzung geistigen Eigentums abgelehnt wird.

Nicht autorisierte Nutzung von urheberrechtlich geschützten Inhalten

Apps, die gegen das Urheberrecht verstoßen, sind nicht zulässig. Auch das Ändern urheberrechtlich geschützter Inhalte schützt nicht unbedingt vor einem Verstoß. Entwickler müssen in der Lage sein, ihr Recht auf Nutzung des urheberrechtlich geschützten Inhalts zu belegen.

Seien Sie vorsichtig, wenn Sie urheberrechtlich geschützte Inhalte verwenden, um die Funktionalität Ihrer App zu demonstrieren. Im Allgemeinen ist es am sichersten, eigene Inhalte zu erstellen.

Da Google Play eine sichere und respektvolle Plattform bleiben soll, haben wir Richtlinien entwickelt, in denen schädliche oder unangemessene Inhalte definiert und verboten werden.

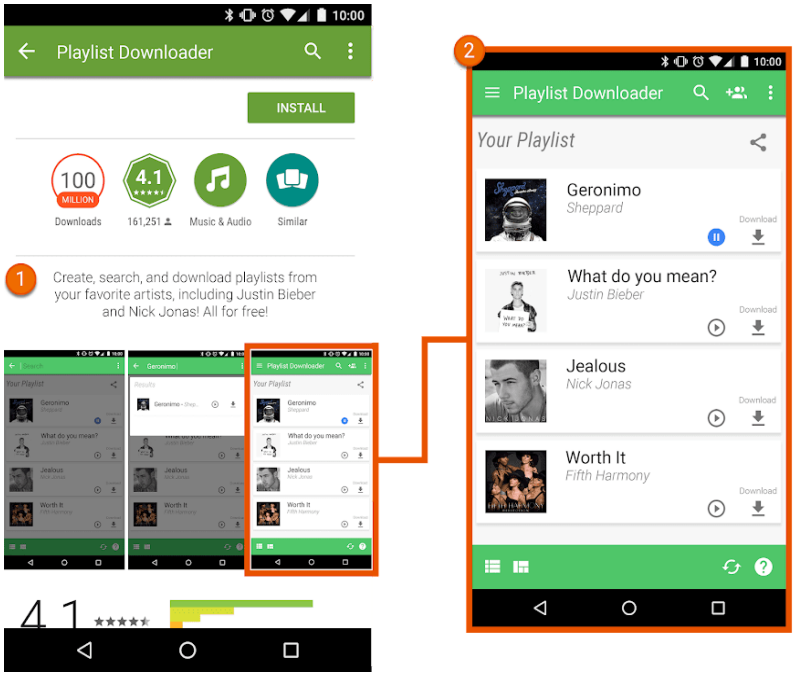
- Covergestaltung für Musikalben, Videospiele und Bücher
- Marketingbilder aus Filmen, Videospielen oder aus dem Fernsehen
- Grafiken oder Bilder aus Comicbüchern, Cartoons, Filmen, Musikvideos oder aus dem Fernsehen
- Logos von College- oder Profimannschaften
- Fotos aus dem Social Media-Konto einer Person des öffentlichen Lebens
- Professionelle Bilder von Personen des öffentlichen Lebens
- Reproduktionen oder Fankunst, die sich vom urheberrechtlich geschützten Original nicht unterscheiden lassen
- Apps mit Soundboards, die Audioclips aus urheberrechtlich geschützten Inhalten abspielen
- Vollständige Reproduktionen oder Übersetzungen von Büchern, die nicht frei von Urheberrechten sind

Anstiftung zur Urheberrechtsverletzung

Apps, die zu Urheberrechtsverletzungen verleiten oder anstiften, sind nicht zulässig. Vor der Veröffentlichung Ihrer App sollten Sie prüfen, ob sie in irgendeiner Weise Urheberrechtsverletzungen begünstigt, und gegebenenfalls juristischen Rat einholen.

Da Google Play eine sichere und respektvolle Plattform bleiben soll, haben wir Richtlinien entwickelt, in denen schädliche oder unangemessene Inhalte definiert und verboten werden.

- Streaming-Apps, mit denen Nutzer verbotenerweise eine lokale Kopie des urheberrechtlich geschützten Inhalts herunterladen können
- Apps, die Nutzer entgegen geltender Urheberrechtsgesetze zum Streamen und Herunterladen urheberrechtlich geschützter Werke verleiten, einschließlich Musik und Videos:



① Der App-Eintrag enthält eine Beschreibung, in der Nutzer zum unerlaubten Download urheberrechtlich geschützter Inhalte angestiftet werden.
② Der App-Eintrag enthält einen Screenshot, der Nutzer zum unerlaubten Download urheberrechtlich geschützter Inhalte anstiftet.

Verletzung des Markenrechts

Apps, die die Markenrechte Dritter verletzen, sind nicht zulässig. Eine Marke ist ein Wort, ein Symbol oder eine Kombination daraus zur Kennzeichnung der Herkunft einer Ware oder Dienstleistung. Nach Erwerb einer Marke erhält der Inhaber die ausschließlichen Rechte an der Markennutzung in Bezug auf bestimmte Waren oder Dienstleistungen.

Bei einer Verletzung des Markenrechts handelt es sich um eine unangemessene oder unbefugte Verwendung einer Marke in einer Weise, die mit großer Wahrscheinlichkeit zu Unklarheiten hinsichtlich der Herkunft des Produkts führt. Wenn Sie in Ihrer App Marken einer anderen Partei in einer Weise verwenden, die wahrscheinlich zu Verwechslungen führt, kann Ihre App gesperrt werden.

Fälschung

Apps, über die Produktfälschungen verkauft oder beworben werden, sind nicht zulässig. Produktfälschungen sind Produkte, die Marken oder Logos enthalten, die mit der Marke bzw. dem Logo eines anderen Anbieters identisch oder kaum davon zu unterscheiden sind. Diese Markenkennzeichen werden nachgeahmt, um den Eindruck zu erwecken, es handle sich um ein echtes Produkt des Markeninhabers.

Datenschutz, Täuschung und Missbrauch von Geräten

Wir legen großen Wert auf Datenschutz und möchten unseren Nutzern eine sichere Umgebung bieten. Irreführende oder schädliche Apps sowie solche, die Netzwerke, Geräte oder personenbezogene Daten in irgendeiner Weise missbrauchen oder zweckentfremden, sind strengstens untersagt.

Nutzerdaten

Sie müssen transparent machen, wie Sie mit Nutzerdaten umgehen (z. B. mit vom Nutzer bereitgestellten Informationen und Informationen, die über einen Nutzer erfasst werden, einschließlich Geräteinformationen). Das bedeutet: Sie müssen den Zugriff auf Nutzerdaten sowie deren Erhebung, Verwendung, Handhabung und Weitergabe durch Ihre App offenlegen und die Verwendung der Daten auf die offengelegten richtlinienkonformen Zwecke beschränken. Beachten Sie, dass die Handhabung personenbezogener und vertraulicher Nutzerdaten auch den zusätzlichen Anforderungen unten im Abschnitt „Personenbezogene und vertrauliche Nutzerdaten“ unterliegt. Die Google Play-Anforderungen gelten zusätzlich zu den Anforderungen der geltenden Datenschutzgesetze.

Wenn in Ihrer App Code von Drittanbietern enthalten ist, etwa ein SDK, müssen Sie sicherstellen, dass dieser in Ihrer App verwendete Code und die Praktiken des Drittanbieters im Hinblick auf Nutzerdaten aus Ihrer App den Google Play-Programmrichtlinien für Entwickler entsprechen, zu denen auch die Verwendungs- und Offenlegungspflichten gehören. So dürfen Ihre SDK-Anbieter beispielsweise keine personenbezogenen und vertraulichen Nutzerdaten aus Ihrer App verkaufen. Diese Anforderung gilt unabhängig davon, ob Nutzerdaten weitergegeben werden, nachdem sie an einen Server gesendet wurden oder indem Drittanbietercode in Ihre App eingebettet wurde.

Personenbezogene und vertrauliche Nutzerdaten

Personenbezogene und vertrauliche Nutzerdaten umfassen unter anderem personenidentifizierbare Informationen, Finanz- und Zahlungsinformationen, Authentifizierungsinformationen, Telefonbuchdaten, Kontakte, den Gerätestandort , SMS- und anrufbezogene Daten,

Gesundheitsdaten , Health Connect-Daten , Informationen darüber, welche anderen Apps auf dem Gerät installiert sind, Mikrofon- und Kameradaten sowie andere vertrauliche Geräte- oder Nutzungsdaten. Wenn Ihre App personenbezogene und vertrauliche Nutzerdaten verarbeitet, müssen Sie Folgendes tun:

- Sie müssen den appseitigen Zugriff auf personenbezogene und vertrauliche Daten sowie deren Erhebung, Verwendung und Weitergabe auf App- und Dienstfunktionen sowie richtlinienkonforme Zwecke beschränken, die vom Nutzer erwartet werden:
  - Apps, in denen personenbezogene und vertrauliche Nutzerdaten außerdem zur Bereitstellung von Werbung verwendet werden, müssen den Werberichtlinien von Google Play entsprechen.
  - Die Weitergabe von Daten nach Bedarf an Dienstanbieter oder aus rechtlichen Gründen ist auch zulässig, etwa zur Erfüllung eines rechtskräftigen behördlichen Ersuchens, zur Einhaltung geltenden Rechts oder im Rahmen einer Fusion oder eines Verkaufs. In diesem Fall müssen die Nutzer angemessen darüber informiert werden.
- Alle personenbezogenen und vertraulichen Nutzerdaten müssen sicher verarbeitet und mit modernen Verschlüsselungsverfahren übertragen werden, z. B. über HTTPS.
- Fragen Sie, wenn möglich, Laufzeitberechtigungen an, bevor Sie über Android-Berechtigungsanfragen auf Daten zugreifen.
- Sie dürfen keine personenbezogenen und vertraulichen Nutzerdaten verkaufen.
  - „Verkauf“ ist der Austausch personenbezogener und vertraulicher Nutzerdaten mit Dritten oder die Weitergabe an solche gegen Bezahlung.
    - Eine durch Nutzer initiierte Weitergabe personenbezogener und vertraulicher Nutzerdaten wird nicht als Verkauf betrachtet. Dazu gehört beispielsweise, wenn Nutzer eine Funktion einer App verwenden, um eine Datei an Dritte zu senden, oder wenn sie sich dafür entscheiden, eine App zu verwenden, die speziell für die Teilnahme an einer Forschungsstudie bestimmt ist.

Pflicht zur deutlichen Offenlegung und Einwilligung

In Fällen, in denen der appseitige Zugriff auf personenbezogene und vertrauliche Nutzerdaten sowie deren Erhebung, Verwendung oder Weitergabe nicht den angemessenen Erwartungen des Nutzers des betreffenden Produkts oder der betreffenden Funktion entsprechen, z. B. wenn die Datenerhebung im Hintergrund stattfindet, während der Nutzer nicht mit der App interagiert, müssen die folgenden Anforderungen erfüllt sein:

Deutliche Offenlegung: In der App muss offengelegt werden, dass Sie auf Daten zugreifen und diese erheben, verwenden und weitergeben. Die Offenlegung innerhalb der App muss folgende Kriterien erfüllen:

- Sie muss in der App selbst und nicht nur in der App-Beschreibung oder auf einer Website angezeigt werden.
- Sie muss dem Nutzer während der normalen Verwendung der App angezeigt werden, ohne dass dieser ein Menü oder Einstellungen öffnen muss.
- Die Art der Daten, auf die zugegriffen wird bzw. die erhoben werden, muss angegeben werden.
- Es muss erklärt werden, wozu die Daten genutzt und/oder weitergegeben werden.
- Die Offenlegung darf nicht nur in der Datenschutzerklärung oder in den Nutzungsbedingungen erfolgen.
- Sie darf nicht in andere Offenlegungen integriert werden, die nicht im Zusammenhang mit der Erhebung personenbezogener und vertraulicher Nutzerdaten stehen.

Einwilligung und Laufzeitberechtigungen: Anfragen zur Nutzereinwilligung und Laufzeitberechtigungsanfragen in der App muss unmittelbar eine Offenlegung in der App vorangehen, die den Anforderungen dieser Richtlinie entspricht. Dabei sind folgende Kriterien zu erfüllen:

- Der Dialog zur Einholung von Einwilligungen muss klar und eindeutig präsentiert werden.

- Der Nutzer muss z. B. durch Tippen oder das Anklicken eines Kästchens aktiv seine Einwilligung bekunden.
- Ein Wegtippen der Offenlegung, das Drücken der Zurück- oder Startbildschirmtaste oder Ähnliches darf nicht als Einwilligung aufgefasst werden.
- Meldungen, die automatisch geschlossen werden oder zeitlich befristet sind, dürfen nicht zum Einholen der Einwilligung des Nutzers verwendet werden.
- Der Nutzer muss seine Einwilligung bekunden, bevor Ihre App damit beginnen kann, personenbezogene und vertrauliche Nutzerdaten zu erheben oder auf diese zuzugreifen.

Apps, für deren Verarbeitung personenbezogener und vertraulicher Nutzerdaten ohne Einwilligung eine andere Rechtsgrundlage gilt, etwa berechtigtes Interesse gemäß der DSGVO der EU, müssen alle anwendbaren rechtlichen Anforderungen erfüllen und Nutzern entsprechende Offenlegungen zur Verfügung stellen, einschließlich In-App-Offenlegungen gemäß den Anforderungen dieser Richtlinie.

Wir empfehlen, die folgenden Beispielformate für die deutliche Offenlegung zu verwenden, um die Richtlinienanforderungen zu erfüllen.

- „[Diese App] erhebt/überträgt/synchronisiert/speichert [Datentyp], um [Funktion] zu ermöglichen, wenn [Szenario]."
- *Beispiel: „Fitness Funds erhebt Standortdaten, um das Fitness-Tracking zu ermöglichen, auch wenn die App geschlossen ist oder nicht verwendet wird. Diese Daten werden auch verwendet, um relevante Werbung anzuzeigen."*
- *Beispiel: „Call Buddy erhebt Anruflistendaten, um das Organisieren von Kontakten zu ermöglichen, auch wenn die App nicht verwendet wird."*

Wenn in Ihrer App Code von Drittanbietern enthalten ist, etwa ein SDK, der dazu dient, standardmäßig personenbezogene und vertrauliche Nutzerdaten zu erheben, müssen Sie innerhalb von zwei Wochen nach Erhalt einer Anfrage von Google Play (oder innerhalb des in der Google Play-Anfrage angegebenen Zeitraums, sofern dort ein anderer Zeitraum angegeben ist) ausreichend nachweisen, dass Ihre App die in dieser Richtlinie beschriebene Pflicht zur deutlichen Offenlegung und Einwilligung erfüllt, etwa im Hinblick auf Datenzugriff sowie Erhebung, Verwendung und Weitergabe von Daten durch Drittanbietercode.

Da Google Play eine sichere und respektvolle Plattform bleiben soll, haben wir Richtlinien entwickelt, in denen schädliche oder unangemessene Inhalte definiert und verboten werden.

- Apps, die Daten zum Gerätestandort erheben und nicht deutlich offenlegen, von welchen Funktionen sie verwendet werden und/oder ob sie im Hintergrund verwendet werden.
- Apps, die über eine Laufzeitberechtigung um Zugriff auf Daten bitten, bevor deutlich offengelegt wird, wie die Daten verwendet werden.
- Apps, die auf das Inventar der installierten Apps eines Nutzers zugreifen und bei denen diese Daten nicht als personenbezogene oder vertrauliche Nutzerdaten gemäß der oben angegebenen Datenschutzerklärung und den Anforderungen hinsichtlich Datenverarbeitung, deutlicher Offenlegung und Zustimmung behandelt werden.
- Apps, die auf die Telefonbuch- oder Kontaktdaten eines Nutzers zugreifen und bei denen diese Daten nicht als personenbezogene oder vertrauliche Nutzerdaten gemäß der oben angegebenen Datenschutzerklärung und den Anforderungen hinsichtlich Datenverarbeitung, deutlicher Offenlegung und Zustimmung behandelt werden.
- Apps, bei denen der Bildschirm des Nutzers aufgezeichnet wird und diese Informationen nicht wie personenbezogene oder vertrauliche Daten, die diesen Richtlinien unterliegen, behandelt werden.
- Apps, die Daten zum Gerätestandort erheben und entgegen den oben stehenden Anforderungen die Nutzung nicht umfassend offenlegen und keine Einwilligung dafür einholen.
- Apps, die eingeschränkte Berechtigungen im Hintergrund verwenden, einschließlich für Tracking-, Recherche- oder Marketingzwecke, und entgegen den oben stehenden Anforderungen die Nutzung nicht umfassend offenlegen und keine Einwilligung dafür einholen.

- Apps mit einem SDK, durch das personenbezogene und vertrauliche Nutzerdaten erhoben werden, das diese Daten aber nicht gemäß dieser Richtlinie zu Nutzerdaten sowie gemäß den Anforderungen an den Zugriff und die Handhabung der Daten (einschließlich des Verkaufsverbots) verarbeitet. Dabei wird auch vom App-Entwickler die Pflicht zur deutlichen Offenlegung und Einwilligung nicht eingehalten.

In diesem Artikel finden Sie weitere Informationen über die Pflicht zur deutlichen Offenlegung und Einwilligung.

Einschränkungen für den Zugriff auf personenbezogene und vertrauliche Daten

Zusätzlich zu den Anforderungen oben gelten für bestimmte Aktivitäten noch weitere Anforderungen, die in der untenstehenden Tabelle erläutert sind.

Aktivität	Anforderung
Verarbeitung von Finanz- oder Zahlungsinformationen oder amtlichen Identifikationsnummern	Unter keinen Umständen darf die App personenbezogene und vertrauliche Nutzerdaten im Zusammenhang mit Finanz- oder Zahlungsaktivitäten oder amtliche Identifikationsnummern offenlegen.
Verarbeitung von nicht öffentlichen Telefonbuch- oder Kontaktdaten	Die unbefugte Veröffentlichung oder Offenlegung von nicht öffentlichen Kontakten der Nutzer ist nicht gestattet.
Virenschutz- oder Sicherheitsfunktionen wie Antiviren-, Anti-Malware- oder sicherheitsbezogene Funktionen	Es ist eine Datenschutzerklärung erforderlich, in der, wie auch in eventuellen Bekanntmachungen in der App selbst, erläutert wird, welche Nutzerdaten erhoben und übertragen werden, wie diese verwendet und an wen sie weitergegeben werden.
Ausrichtung auf Kinder	Die App darf kein SDK enthalten, das nicht für die Verwendung in Diensten für Kinder zugelassen ist. Vollständige Informationen zu Richtlinienformulierungen und -anforderungen finden Sie unter Apps für Kinder und Familien .
Erhebung oder Verknüpfung gleichbleibender Geräte-IDs, z. B. IMEIs, IMSIs und SIM-Seriennummern	Gleichbleibende Geräte-IDs dürfen nicht mit anderen personenbezogenen und vertraulichen Nutzerdaten oder zurücksetzbaren Geräte-IDs verknüpft werden, mit folgenden Ausnahmen: • Zu Telefoniezwecken in Verbindung mit einer SIM-Identität, z. B. bei Anrufen über WLAN, die mit einem Mobilfunkanbieter-Konto verknüpft sind • Bei Apps zur Verwaltung von Unternehmensgeräten im Geräte-Eigentümermodus Diese Verwendungszwecke müssen für Nutzer entsprechend den Richtlinien zu Nutzerdaten deutlich sichtbar angebracht sein. In dieser Ressource finden Sie Informationen zu alternativen eindeutigen Kennzeichnungen. In der Werberichtlinie finden Sie zusätzliche Informationen zur Android-Werbe-ID.

Abschnitt zur Datensicherheit

Alle Entwickler müssen für jede App den Abschnitt zur Datensicherheit verständlich und wahrheitsgemäß ausfüllen. Dabei sind die Erhebung, Verwendung und Weitergabe von Nutzerdaten umfassend offenzulegen. Der Entwickler ist für die Richtigkeit der Angaben im Abschnitt zur Datensicherheit und die laufende Aktualisierung dieser Informationen verantwortlich. Sofern relevant muss der Abschnitt den Offenlegungen in der Datenschutzerklärung der App entsprechen.

Hier finden Sie zusätzliche Informationen zum Ausfüllen des Abschnitts zur Datensicherheit.

Datenschutzerklärung

Für alle Apps muss im dafür vorgesehenen Feld in der Play Console ein Link zur Datenschutzerklärung sowie in der App selbst ein Link zur Datenschutzerklärung oder die Datenschutzerklärung in Textform veröffentlicht werden. In der Erklärung sowie in Offenlegungen in der App selbst muss umfassend offengelegt werden, wie durch die App auf Nutzerdaten zugegriffen wird und wie diese Daten erhoben, verwendet und weitergegeben werden. Dies beschränkt sich nicht auf die Daten, die im Abschnitt zur Datensicherheit beschrieben werden. Diese Offenlegung muss Folgendes beinhalten:

- Informationen zum Entwickler und einen Ansprechpartner bei Fragen zum Datenschutz oder eine Möglichkeit, Anfragen zu stellen.
- Eine Beschreibung der Arten von personenbezogenen und vertraulichen Nutzerdaten, auf die Ihre App zugreift, die sie erhebt, verwendet und weitergibt, sowie etwaige Parteien, mit denen personenbezogene oder vertrauliche Nutzerdaten geteilt werden können.
- Sichere Datenverarbeitungsverfahren für personenbezogene und vertrauliche Nutzerdaten.
- Die Richtlinie des Entwicklers zur Datenaufbewahrung und Datenlöschung.
- Eine deutliche Kennzeichnung als Datenschutzerklärung, z. B. durch die Nennung von „Datenschutzerklärung“ im Titel.

In der Datenschutzerklärung muss das Rechtssubjekt, das im Google Play Store-Eintrag genannt wird (z. B. Entwickler oder Unternehmen), oder der App-Titel aufgeführt werden. Auch für Apps, die nicht auf personenbezogene und vertrauliche Nutzerdaten zugreifen, muss eine Datenschutzerklärung vorhanden sein.

Die Datenschutzerklärung muss über eine aktive, öffentlich zugängliche URL verfügbar sein, bei der kein Geofencing eingesetzt wird, die keine PDF ist und die nicht bearbeitet werden kann.

Nutzung der Set-ID der App

In Android wird eine neue ID eingeführt, um wichtige Anwendungsfälle wie Analysen und Betrugsprävention zu ermöglichen. Die Bedingungen für die Nutzung dieser ID finden Sie unten.

- **Verwendung**: Die Set-ID der App darf weder für personalisierte Werbung noch für die Anzeigenmessung verwendet werden.
- **Verknüpfung mit personenidentifizierbaren Informationen oder anderen IDs**: Die App-Set-ID darf nicht für Werbezwecke mit Android-IDs (z. B. AAID) oder personenbezogenen und sensiblen Daten verknüpft werden.
- **Transparenz und Einwilligung**: Die Erhebung und Nutzung dieser Set-ID der App sowie die Verpflichtung zur Einhaltung dieser Bestimmungen muss den Nutzern in einer rechtlich angemessenen Benachrichtigung zum Datenschutz, in der auch Ihre Datenschutzerklärung enthalten ist, mitgeteilt werden. Sie sind verpflichtet, überall dort, wo dies erforderlich ist, eine rechtswirksame Einwilligung der Nutzer einzuholen. Weitere Informationen zu unseren Datenschutzstandards finden Sie in unseren Richtlinien zu Nutzerdaten .

EU-U.S. Privacy Shield (EU-US-Datenschutzschild) und Swiss-U.S. Privacy Shield (CH-US-Datenschutzschild)

Wenn Sie auf von Google zur Verfügung gestellte personenbezogene Daten zugreifen, diese verwenden oder verarbeiten, durch diese Daten eine Person direkt oder indirekt identifiziert werden kann und diese Daten aus der Europäischen Union oder der Schweiz stammen („personenbezogene Daten aus der EU“), gilt Folgendes:

- Sie müssen alle geltenden Gesetze, Richtlinien, Verordnungen und Bestimmungen zum Datenschutz und zur Datensicherheit einhalten.
- Der Zugriff, die Verwendung und die Verarbeitung personenbezogener Daten aus der EU ist nur zu den Zwecken zulässig, denen die entsprechende Person zugestimmt hat.
- Sie sind verantwortlich für organisatorische und technische Maßnahmen zum Schutz der personenbezogenen Daten aus der EU vor Verlust, Missbrauch, unautorisiertem oder

gesetzeswidrigem Zugriff sowie unautorisierter oder gesetzeswidriger Offenlegung, Veränderung und Vernichtung.
- Sie müssen dasselbe Maß an Datenschutz gewährleisten, das in den Privacy-Shield-Prinzipien gefordert wird.

Sie müssen die Einhaltung dieser Verpflichtungen regelmäßig prüfen. Sollten Sie diese Bedingungen nicht mehr erfüllen können oder sollte diesbezüglich ein erhebliches Risiko bestehen, müssen Sie uns sofort per E-Mail an data-protection-office@google.com darüber informieren und die Verarbeitung personenbezogener Daten aus der EU entweder mit sofortiger Wirkung einstellen oder umgehend andere angemessene und geeignete Maßnahmen ergreifen, um ein ausreichendes Datenschutzniveau zu gewährleisten.

Seit dem 16. Juli 2020 greift Google bei der Übermittlung von personenbezogenen Daten aus dem Europäischen Wirtschaftsraum oder dem Vereinigten Königreich in die Vereinigten Staaten nicht mehr auf das EU-U.S. Privacy Shield (EU-US-Datenschutzschild) zurück. Weitere Informationen Weitere Informationen finden Sie in Abschnitt 9 der Vertriebsvereinbarung für Entwickler.

Berechtigungen und APIs, die auf vertrauliche Informationen zugreifen

Anfragen für Berechtigungen und APIs, durch die auf vertrauliche Informationen zugegriffen wird, sollten für die Nutzer Sinn ergeben. Sie dürfen lediglich Anfragen zu Berechtigungen und APIs stellen, über die auf vertrauliche Informationen zugegriffen wird, wenn diese Berechtigungen oder APIs zur Implementierung vorhandener Funktionen oder Dienste in Ihrer App erforderlich sind. Die Funktionen und Dienste müssen in Ihrem Google Play-Eintrag angegeben sein. Berechtigungen oder APIs, über die auf vertrauliche Informationen zugegriffen wird und die den Zugriff auf Nutzer- oder Gerätedaten für nicht offengelegte, nicht implementierte oder nicht zugelassene Funktionen oder Zwecke ermöglichen, dürfen nicht verwendet werden. Personenbezogene oder vertrauliche Daten, auf die über Berechtigungen oder APIs zugegriffen wird, dürfen niemals verkauft oder für einen Zweck weitergegeben werden, der den Verkauf möglich macht.

Anfragen zu Berechtigungen und APIs für den Zugriff auf vertrauliche Informationen sollten möglichst im Kontext, d. h. schrittweise, erfolgen, damit die Nutzer verstehen, weshalb Ihre App die Berechtigungen benötigt. Sie dürfen die Daten nur für Zwecke verwenden, denen der Nutzer zugestimmt hat. Wenn Sie die Daten später für andere Zwecke verwenden möchten, müssen Sie die Zustimmung des Nutzers einholen.

Eingeschränkte Berechtigungen

Neben den oben genannten Berechtigungen gibt es noch eingeschränkte Berechtigungen, die als gefährlich , speziell oder signaturbasiert bzw. wie unten beschrieben gekennzeichnet werden. Für diese Berechtigungen gelten die folgenden zusätzlichen Anforderungen und Einschränkungen:

- Nutzer- oder Gerätedaten, auf die über eingeschränkte Berechtigungen zugegriffen wird, werden als personenbezogene und vertrauliche Nutzerdaten betrachtet. Es gelten die Anforderungen der Richtlinie zu Nutzerdaten .
- Wenn Nutzer die Anforderung einer eingeschränkten Berechtigung ablehnen, muss diese Entscheidung respektiert werden. Ihre Zustimmung zu nicht dringend erforderlichen Berechtigungen darf nicht erzwungen oder beeinflusst werden. Sie müssen Nutzern, die den Zugriff auf vertrauliche Berechtigungen verweigern, so weit wie möglich entgegenkommen. Wenn ein Nutzer den Zugriff auf die Anrufliste zum Beispiel eingeschränkt hat, sollten Sie ihm die Möglichkeit geben, Telefonnummern manuell einzugeben.
- Eine Verwendung von Berechtigungen, die gegen die Google Play-Richtlinie zu Malware verstößt, darunter den Abschnitt zum Missbrauch von erhöhten Berechtigungen , ist explizit verboten.

Bestimmte eingeschränkte Berechtigungen können den weiter unten aufgeführten zusätzlichen Anforderungen unterliegen. Diese Einschränkungen dienen dem Datenschutz unserer Nutzer. In sehr seltenen Fällen, in denen Apps eine besonders interessante oder wichtige Funktion bieten, für deren Bereitstellung es noch keine Alternative gibt, machen wir dabei unter Umständen begrenzte Ausnahmen. Wir wägen dann die vorgeschlagenen Ausnahmen und die potenziellen Auswirkungen auf den Datenschutz oder die Sicherheit für Nutzer gegeneinander ab.

Berechtigungen "SMS" und "Anrufliste"

Die Berechtigungen "SMS" und "Anrufliste" gelten als personenbezogene und vertrauliche Nutzerdaten, die der Richtlinie Personenbezogene und vertrauliche Informationen sowie den folgenden Einschränkungen unterliegen:

Eingeschränkte Berechtigung	Anforderung
Berechtigungsgruppe "Anrufliste" (z. B. READ_CALL_LOG, WRITE_CALL_LOG, PROCESS_OUTGOING_CALLS)	Die App muss aktiv als standardmäßiger Telefon- oder Assistant-Handler auf dem Gerät registriert sein.
Berechtigungsgruppe "SMS" (z. B. READ_SMS, SEND_SMS, WRITE_SMS, RECEIVE_SMS, RECEIVE_WAP_PUSH, RECEIVE_MMS)	Die App muss aktiv als standardmäßiger SMS- oder Assistant-Handler auf dem Gerät registriert sein.

Bei Apps ohne standardmäßige SMS-, Telefon- oder Assistant-Handler-Funktion darf die Nutzung der oben genannten Berechtigungen nicht in der Manifest-Datei deklariert werden. Dies schließt Platzhaltertext in der Manifest-Datei ein. Außerdem muss eine App aktiv als standardmäßiger SMS-, Telefon- oder Assistant-Handler registriert sein, bevor Nutzer durch die App aufgefordert werden, eine der oben genannten Berechtigungen zu gewähren. Die Verwendung der Berechtigung muss sofort eingestellt werden, wenn die App nicht mehr der Standard-Handler ist. Informationen zu den zulässigen Verwendungszwecken und Ausnahmen finden Sie auf dieser Hilfeseite .

In Apps dürfen die Berechtigung und alle aus der Berechtigung abgeleiteten Daten nur verwendet werden, um genehmigte Hauptfunktionen bereitzustellen. Die Hauptfunktionen sind definiert als wesentlicher Zweck der App. Sie können eine Reihe wichtiger Funktionen umfassen, die alle in der Beschreibung der App hervorgehoben werden müssen. Ohne diese wichtigen Funktionen ist die App "defekt" oder unbrauchbar. Die Übertragung, Weitergabe oder lizenzierte Nutzung dieser Daten darf nur zur Bereitstellung von Hauptfunktionen oder -diensten innerhalb der App erfolgen. Die Daten dürfen nicht für andere Zwecke verwendet werden, z. B. zur Optimierung anderer Apps oder Dienste oder zu Werbe- oder Marketingzwecken. Sie dürfen Daten, die den Berechtigungen "SMS" oder "Anrufliste" zugeordnet sind, nicht über alternative Methoden abrufen, einschließlich anderer Berechtigungen, APIs oder Quellen von Drittanbietern.

Berechtigungen zur Standortermittlung

Informationen zum Gerätestandort gelten als persönliche und vertrauliche Nutzerdaten, die der Richtlinie zu personenbezogenen und vertraulichen Informationen und der Richtlinie zur Standortermittlung im Hintergrund sowie den folgenden Einschränkungen unterliegen:

- Apps dürfen auf Daten, die durch Berechtigungen zur Standortermittlung (z. B. ACCESS_FINE_LOCATION, ACCESS_COARSE_LOCATION, ACCESS_BACKGROUND_LOCATION) geschützt sind, nur solange zugreifen, wie dies zur Bereitstellung vorhandener Funktionen oder Dienste in der App erforderlich ist.
- Fordern Sie keine Berechtigungen zur Standortermittlung an, wenn die Daten ausschließlich Werbe- oder Analysezwecken dienen. Apps, bei denen die zulässige Nutzung dieser Daten auf die Schaltung von Werbung ausgeweitet wird, müssen unseren Werberichtlinien entsprechen.
- Zur Bereitstellung vorhandener Funktionen oder Dienste, für die eine Standortermittlung nötig ist, sollten Berechtigungen nur im dafür erforderlichen Mindestumfang angefordert werden – d. h. eine

niedrigere statt hohe Genauigkeit und Vordergrund- statt Hintergrundzugriff. Die Nutzer sollten damit rechnen können, dass die Standortermittlung für die Funktion oder den Dienst im geforderten Umfang benötigt wird. Unter Umständen lehnen wir beispielsweise Apps ab, bei denen ohne triftigen Grund eine Berechtigung zur Standortermittlung im Hintergrund angefordert wird.
- Die Standortermittlung im Hintergrund darf nur in Verbindung mit der Bereitstellung von Funktionen erfolgen, die für den Nutzer von Vorteil und für die Hauptfunktion der App relevant sind.

Apps dürfen unter den nachfolgenden Bedingungen über den Dienst im Vordergrund (wenn die App Vordergrundzugriff hat, also gerade verwendet wird) auf den Standort zugreifen:

- Die Nutzung wurde infolge einer vom Nutzer initiierten Aktion in der App eingeleitet und
- wird, nachdem der Bestimmungszweck der vom Nutzer initiierten Aktion durch die App erfüllt ist, sofort beendet.

Apps, die speziell für Kinder entwickelt wurden, müssen den Designed for Families -Richtlinien entsprechen.

Weitere Informationen zu den Richtlinienanforderungen finden Sie in diesem Hilfeartikel .

Berechtigung „Zugriff auf alle Dateien“

Dateien und Verzeichnisattribute auf dem Gerät eines Nutzers gelten gemäß den Richtlinien für personenbezogene und vertrauliche Informationen und den folgenden Anforderungen als personenbezogene und vertrauliche Nutzerdaten:

- Apps dürfen nur in dem Umfang Zugriff auf den Gerätespeicher anfordern, wie er für die Funktion der App entscheidend ist, und dürfen nicht im Namen eines Drittanbieters Zugriff auf den Gerätespeicher anfordern, der nicht in Zusammenhang mit wichtigen Funktionen für den Nutzer steht.
- Android-Geräte mit R oder höher benötigen die Berechtigung MANAGE_EXTERNAL_STORAGE , um den Zugriff auf den freigegebenen Speicher zu verwalten. Alle Apps, die auf R ausgerichtet sind und einen umfassenden Zugriff auf freigegebenen Speicher („Zugriff auf alle Dateien“) anfordern, müssen vor der Veröffentlichung eine entsprechende Zugriffsüberprüfung bestehen. Apps, die diese Berechtigung verwenden dürfen, müssen Nutzer eindeutig dazu auffordern, unter den Einstellungen für „Spezieller App-Zugriff“ die Option „Zugriff auf alle Dateien“ für ihre App zu aktivieren. Weitere Informationen zu den R-Anforderungen finden Sie in diesem Hilfeartikel .

Berechtigung für die Sichtbarkeit von Paketen (Apps)

Der Bestand installierter Apps, der von einem Gerät abgerufen wird, zählt zu den personenbezogenen und vertraulichen Nutzerdaten, die den Richtlinien zu personenbezogenen und vertraulichen Informationen sowie den folgenden Anforderungen unterliegen:

Apps, deren Hauptzweck darin besteht, andere Apps auf dem Gerät zu starten, zu suchen oder mit ihnen zu interagieren, können Informationen darüber erhalten, welche anderen Apps auf dem Gerät installiert sind. Im Folgenden ist beschrieben, in welchem Umfang dies jeweils möglich ist:

- **Umfassende App-Sichtbarkeit**: Die App kann umfassende Informationen darüber erlangen, welche Apps („Pakete“) auf einem Gerät installiert sind.
  - Für Apps, die auf API-Level 30 oder höher ausgerichtet sind, ist die Sichtbarkeit der installierten Apps über die Berechtigung QUERY_ALL_PACKAGES auf Anwendungsfälle beschränkt, bei denen die Kenntnis von und/oder Interoperabilität mit allen Apps auf dem Gerät erforderlich ist, damit die App funktioniert.
    - Sie dürfen QUERY_ALL_PACKAGES nicht verwenden, wenn Ihre App mit einer Deklaration für eine stärker bereichsspezifische Paketsichtbarkeit funktioniert. Dies ist beispielsweise der Fall, wenn es ausreicht, bestimmte Pakete abzufragen und mit diesen zu interagieren statt eine umfassende Sichtbarkeit anzufordern.

- Die Verwendung alternativer Methoden, um die mit der Berechtigung QUERY_ALL_PACKAGES verknüpfte umfassende Sichtbarkeit zu erlangen, ist ebenfalls darauf beschränkt, die für die Nutzer bestimmten Hauptfunktionen der App auszuführen und die Interoperabilität mit den gefundenen Apps zu gewährleisten.
- In diesem Hilfeartikel finden Sie zulässige Anwendungsfälle für die Berechtigung QUERY_ALL_PACKAGES.

- **Eingeschränkte App-Sichtbarkeit**: Die App greift nur auf wenige Daten zu, indem anstelle einer umfassenden eine spezifische Suche nach Apps durchgeführt wird, z. B. nach Apps, die die Manifestdeklaration der App erfüllen. Sie können diese Methode für die Abfrage von Apps verwenden, wenn Ihre App richtlinienkonforme Interoperabilität aufweist oder diese Apps verwaltet.
- Die Sichtbarkeit installierter Apps auf einem Gerät muss direkt erforderlich sein, um den Hauptzweck der App erfüllen bzw. dem Nutzer die Hauptfunktionen anbieten zu können.

Daten, die über den Bestand von Apps, die über den Play Store vertrieben werden, abgerufen werden, dürfen weder verkauft noch anderweitig weitergegeben werden, sei es für die Analyse oder die Anzeigenmonetarisierung.

Accessibility API

Die Accessibility API darf für Folgendes nicht verwendet werden:

- Hindern der Nutzer, die App oder den Dienst zu deaktivieren oder zu deinstallieren, oder Ändern von Nutzereinstellungen ohne Einwilligung des Nutzers, es sei denn, dies wurde durch einen Elternteil oder Erziehungsberechtigten über eine Jugendschutz-App autorisiert oder von autorisierten Administratoren über eine Unternehmenssoftware vorgenommen
- Umgehen der in Android integrierten Datenschutzeinstellungen und -benachrichtigungen
- Ändern oder Verwenden der Benutzeroberfläche auf irreführende Weise oder entgegen den Google Play-Richtlinien für Entwickler

Die Accessibility API ist nicht für die Aufzeichnung von Ferngesprächen vorgesehen. Entsprechende Anfragen können nicht gestellt werden.

Die Nutzung der Accessibility API muss im Google Play-Eintrag dokumentiert sein.

Richtlinien für das IsAccessibilityTool

Für Apps, deren Hauptfunktionen Menschen mit Behinderung direkt unterstützen sollen, darf das Attribut **IsAccessibilityTool** genutzt werden, um sie offiziell als Bedienungshilfen-App auszuweisen.

Für Apps, für die die Verwendung des **IsAccessibilityTool** nicht vorgesehen ist, darf diese Bezeichnung nicht genutzt werden. Sie müssen die Anforderungen zur deutlichen Offenlegung und Zustimmung gemäß den Richtlinien zu Nutzerdaten erfüllen, da ihre Bedienungshilfefunktionen für den Nutzer nicht offensichtlich sind. Weitere Informationen finden Sie im Hilfeartikel Verwendung der AccessibilityService API .

Wann immer möglich sollten für Apps nur die für die gewünschten Funktionsweisen wirklich notwendigen APIs und Berechtigungen mit begrenztem Zugriff anstelle der Accessibility API verwendet werden.

Berechtigung für die Anfrage zur Installation von Paketen

Mit der Berechtigung REQUEST_INSTALL_PACKAGES kann eine App die Installation von App-Paketen anfordern. Um diese Berechtigung zu nutzen, muss die App folgende Hauptfunktionen umfassen:

- App-Pakete senden oder empfangen
- Vom Nutzer initiierte Installation von App-Paketen ermöglichen

Zulässige Funktionen:

- Surfen oder Suche im Web
- Kommunikationsdienste, die Anhänge unterstützen
- Freigabe, Weiterleitung oder Verwaltung von Dateien
- Geräteverwaltung für Unternehmen
- Back-up und Wiederherstellung
- Gerätemigration/Datenübertragung von Smartphones
- Companion-App zur Synchronisierung von Smartphone und Wearable oder IoT-Gerät (beispielsweise Smartwatch oder Smart-TV)

Die Hauptfunktionen sind als wesentlicher Zweck der App definiert. Die Hauptfunktionen sowie alle wesentlichen Merkmale, die diese Funktionen ausmachen, müssen in der Beschreibung der App deutlich herausgestellt und beworben werden.

Die Berechtigung REQUEST_INSTALL_PACKAGES darf nicht verwendet werden, um andere APKs selbst zu aktualisieren, zu ändern oder in der Asset-Datei zu bündeln, es sei denn, dies dient der Geräteverwaltung. Alle Aktualisierungen oder Installationen von Paketen müssen der Richtlinie zum Missbrauch von Geräten und Netzwerken von Google Play entsprechen und vom Nutzer initiiert und ausgeführt werden.

Berechtigungen für Health Connect by Android

Daten, auf die unter Verwendung von Berechtigungen für Health Connect zugegriffen wird, werden als personenbezogene und vertrauliche Nutzerdaten erachtet, die der Richtlinie zu Nutzerdaten und den folgenden zusätzlichen Anforderungen unterliegen:

Berechtigter Zugriff auf und berechtigte Nutzung von Health Connect

Anfragen bezüglich des Zugriffs auf Daten über Health Connect-Berechtigungen müssen klar und verständlich formuliert sein. Health Connect darf nur gemäß den geltenden Richtlinien und Nutzungsbedingungen und nur für die in der vorliegenden Richtlinie erläuterten genehmigten Anwendungsfälle verwendet werden. Das bedeutet, dass Sie nur dann Zugriff auf Berechtigungen anfordern dürfen, wenn Ihre App oder Ihr Dienst einem der genehmigten Anwendungsfälle entspricht.

Genehmigte Anwendungsfälle für den Zugriff auf Health Connect-Berechtigungen sind:

- Apps oder Dienste, in denen eine oder mehrere Funktionen zur Förderung der Gesundheit und Fitness von Nutzern in einer Benutzeroberfläche zur Verfügung gestellt werden, um diesen Nutzern zu ermöglichen, ihre körperlichen Aktivitäten, ihren Schlaf, ihr geistiges Wohlbefinden, ihre Ernährungsgewohnheiten, ihre Gesundheitsdaten, ihre Körpermaße und/oder andere Gesundheits- oder Fitnessinformationen oder -messdaten direkt **aufzuzeichnen, zu melden, zu beobachten und/oder zu analysieren**.
- Apps oder Dienste, in denen eine oder mehrere Funktionen zur Förderung der Gesundheit und Fitness von Nutzern in einer Benutzeroberfläche zur Verfügung gestellt werden, um diesen Nutzern zu ermöglichen, ihre körperlichen Aktivitäten, ihren Schlaf, ihr geistiges Wohlbefinden, ihre Ernährungsgewohnheiten, ihre Gesundheitsdaten, ihre Körpermaße und/oder andere Gesundheits- oder Fitnessinformationen oder -messdaten auf ihrem Smartphone und/oder Wearable **zu speichern** und diese Daten für andere Apps auf dem Gerät freizugeben, die diesen Anwendungsfällen entsprechen.

Health Connect ist eine Mehrzweckplattform zum Speichern und Teilen von Daten, die es Nutzern ermöglicht, Gesundheits- und Fitnessdaten von unterschiedlichen Quellen auf ihrem Android-Gerät zu erfassen und zusammenzufassen und sie nach eigenem Ermessen mit Dritten zu teilen. Die Daten können aus unterschiedlichen Quellen stammen, die von den Nutzern selbst bestimmt werden können. Entwickler müssen beurteilen, ob Health Connect für ihre beabsichtigte Nutzung geeignet ist, und die Quelle und Qualität der Daten in Health Connect im Zusammenhang mit dem jeweiligen Zweck analysieren und prüfen, insbesondere für den Einsatz im Forschungs-, Gesundheits- oder medizinischen Bereich.

- Für Apps, mit denen Untersuchungen der menschlichen Gesundheit mithilfe von Daten durchgeführt werden, die von Health Connect stammen, muss die Einwilligung der Teilnehmer oder, im Fall von Minderjährigen, der Eltern oder Erziehungsberechtigten eingeholt werden. Eine solche Einwilligung muss folgende Informationen enthalten: (a) Art, Zweck und Dauer der Untersuchung, (b) Verfahren, Risiken und Nutzen für den Teilnehmer, (c) Informationen über die Vertraulichkeit und die Handhabung von Daten (einschließlich der etwaigen Weitergabe an Dritte), (d) eine Kontaktperson für Fragen des Teilnehmers und (e) das Widerrufsverfahren. Apps, mit denen Untersuchungen der menschlichen Gesundheit mithilfe von Daten durchgeführt werden, die von Health Connect stammen, erfordern die Genehmigung durch eine unabhängige Stelle, die 1) die Rechte, die Sicherheit und das Wohlergehen der Teilnehmer schützt und 2) die Befugnis hat, die Untersuchungen am Menschen zu prüfen, zu ändern und zu genehmigen. Auf Anfrage muss ein Nachweis dieser Genehmigung vorgelegt werden.
- Darüber hinaus sind Sie dafür verantwortlich, alle behördlichen oder gesetzlichen Vorschriften einzuhalten, die für Ihre beabsichtigte Nutzung von Health Connect und von aus Health Connect stammenden Daten gelten. Sofern nicht ausdrücklich in der Kennzeichnung oder in den von Google bereitgestellten Informationen zu bestimmten Google-Produkten oder -Diensten angegeben, empfiehlt Google nicht die Verwendung der in Health Connect gespeicherten Daten für einen bestimmten Anwendungsfall oder einen bestimmten Zweck, insbesondere für die Nutzung in der Forschung, im Gesundheitswesen oder in der Medizin, und übernimmt auch keine Garantie für die Korrektheit der darin enthaltenen Daten. Google lehnt jegliche Haftung in Verbindung mit der Verwendung der über Health Connect erhaltenen Daten ab.

Eingeschränkte Nutzung

Zusätzlich zur Nutzung von Health Connect für einen rechtmäßigen Zweck muss Ihre Nutzung der von Health Connect stammenden Daten auch die folgenden Anforderungen erfüllen. Diese Anforderungen beziehen sich auf die von Health Connect stammenden Rohdaten sowie die Daten, die mithilfe der Rohdaten zusammengestellt, de-identifiziert oder abgeleitet werden.

- Beschränken Sie die Verwendung von Health Connect-Daten auf die Bereitstellung oder Verbesserung desjenigen Anwendungsfalls oder derjenigen Funktionen, die in der Benutzeroberfläche der anfragenden App deutlich sichtbar sind.
- Übertragen Sie Nutzerdaten nur aus folgenden Gründen an Dritte:
  - Zur Bereitstellung oder Verbesserung desjenigen Anwendungsfalls oder derjenigen Funktionen, der/die in der Benutzeroberfläche der anfragenden App deutlich sichtbar ist/sind, wobei die Übertragung nur mit Einwilligung der Nutzer erfolgen darf
  - Falls dies aus Sicherheitsgründen erforderlich ist (beispielsweise zur Untersuchung von Missbrauch)
  - Zur Einhaltung geltender Gesetze und/oder Vorschriften
  - Im Rahmen einer Fusion, eines Erwerbs oder einer Veräußerung von Vermögenswerten des Entwicklers, nachdem zuvor vom Nutzer seine ausdrückliche Einwilligung eingeholt wurde
- Gestatten Sie Personen nicht, Nutzerdaten zu lesen, es sei denn:
  - Es wird die ausdrückliche Einwilligung des Nutzers zum Lesen bestimmter Daten eingeholt
  - Es ist aus Sicherheitsgründen erforderlich (beispielsweise zur Untersuchung von Missbrauch)
  - Es ist zur Einhaltung geltender Gesetze erforderlich
  - Die Daten (einschließlich abgeleiteter Daten) werden gemäß den geltenden Datenschutzvorschriften und anderen rechtlichen Anforderungen der jeweiligen Gerichtsbarkeit aggregiert und für interne Vorgänge verwendet

Alle anderen Formen der Übertragung, der Verwendung oder des Verkaufs von Health Connect-Daten sind untersagt. Hierzu zählen auch:

- Die Übertragung oder der Verkauf von Nutzerdaten an Dritte wie beispielsweise Werbeplattformen, Datenbroker oder Wiederverkäufer von Informationen

- Die Übertragung, der Verkauf oder die Verwendung von Nutzerdaten für die Schaltung von Werbeanzeigen, einschließlich personalisierter oder interessenbezogener Werbung
- Die Übertragung, der Verkauf oder die Verwendung von Nutzerdaten zur Ermittlung der Kreditwürdigkeit oder zu Kreditvergabezwecken
- Die Übertragung oder der Verkauf von Nutzerdaten an oder die Verwendung von Nutzerdaten mit einem Produkt oder Dienst, das/der als Medizinprodukt gemäß Paragraf 201(h) des Federal Food, Drug, and Cosmetic Act erachtet werden kann, wenn die Nutzerdaten vom Medizinprodukt zur Durchführung seiner zugelassenen Funktion verwendet werden
- Die Übertragung, der Verkauf oder die Verwendung von Nutzerdaten, die „geschützte Gesundheitsdaten" (Protected Health Information, PHI) beinhalten (gemäß der Definition im HIPAA), zu einem beliebigen Zweck oder auf eine beliebige Art, es sei denn, Sie erhalten von Google eine vorherige schriftliche Genehmigung zu einer solchen Verwendung

Der Zugriff auf Health Connect ist untersagt, wenn gegen diese Richtlinie oder andere geltende Health Connect-Nutzungsbedingungen oder -Richtlinien verstoßen wird, und auch in den folgenden Fällen:

- Verwenden Sie Health Connect nicht zur Entwicklung oder zur Einbindung in Anwendungen, Umgebungen oder Aktivitäten, bei denen vernünftigerweise angenommen werden kann, dass die Nutzung oder der Ausfall von Health Connect zum Tod, zu Personenschäden oder zu Umwelt- oder Sachschäden führen kann (wie beispielsweise beim Bau oder Betrieb von kerntechnischen Anlagen, Flugsicherungsanlagen, lebenserhaltenden Systemen oder Waffensystemen).
- Greifen Sie nicht über Headless-Apps auf Daten zu, die Sie über Health Connect erhalten haben. Apps müssen ein deutlich erkennbares Symbol u. a. für die App-Ablage, App-Einstellungen und Benachrichtigungssymbole haben.
- Verwenden Sie Health Connect nicht mit Apps, durch die Daten zwischen inkompatiblen Geräten oder Plattformen synchronisiert werden.
- Health Connect kann nicht mit Apps, Diensten oder Funktionen verbunden werden, die sich ausschließlich an Kinder richten. Health Connect ist nicht für die Verwendung in Diensten genehmigt, die vorwiegend auf Kinder ausgerichtet sind.

In Ihrer App oder auf einer Website, die zu Ihrem Webdienst oder Ihrer App gehört, muss eine Bestätigung zu sehen sein, in der versichert wird, dass Ihre Verwendung von Health Connect-Daten den Anforderungen bezüglich der eingeschränkten Datennutzung entspricht. Das könnte beispielsweise ein Link auf einer Startseite sein, der zu einer speziellen Seite oder einer Datenschutzerklärung führt und folgenden Hinweis enthält: „Die Verwendung der von Health Connect erhaltenen Daten entspricht der Richtlinie zu Berechtigungen für Health Connect, einschließlich den Anforderungen bezüglich der eingeschränkten Nutzung."

Mindestumfang

Sie dürfen nur Zugriff auf Berechtigungen fordern, die unbedingt für die Implementierung der Funktionen Ihrer App oder Ihres Dienstes erforderlich sind.

Das bedeutet:

- Fordern Sie keinen Zugriff auf Informationen an, die Sie nicht benötigen. Fordern Sie nur Zugriff auf die Berechtigungen an, die für die Implementierung der Funktionen oder Dienste Ihres Produkts erforderlich sind. Wenn Ihr Produkt keinen Zugriff auf spezifische Berechtigungen erfordert, dürfen Sie keinen Zugriff auf diese Berechtigungen anfordern.

Transparente und genaue Information und Kontrolle

Health Connect handhabt Gesundheits- und Fitnessdaten, die personenbezogene und vertrauliche Informationen beinhalten. Alle Apps und Dienste müssen eine Datenschutzrichtlinie haben, in der detailliert erläutert wird, wie eine App oder ein Dienst Nutzerdaten erfasst, nutzt und weitergibt. Hierzu gehören auch die Arten von Dritten, an die etwaige Nutzerdaten weitergegeben werden, wie Sie die

Daten nutzen, wie Sie die Daten speichern und sichern und was mit den Daten passiert, wenn ein Konto deaktiviert und/oder gelöscht wird.

Zusätzlich zu den gesetzlichen Anforderungen müssen Sie auch folgende Anforderungen erfüllen:

- Sie müssen Informationen über den Zugriff auf die Daten und deren Erfassung, Nutzung und Weitergabe offenlegen. In der Offenlegung:
  - Muss die Identität der App oder des Dienstes, über den auf Nutzerdaten zugegriffen wird, korrekt angegeben sein.
  - Müssen genaue und korrekte Informationen zu den Typen von Daten, auf die zugegriffen wird und die angefordert und/oder erfasst werden, angegeben sein.
  - Muss erklärt werden, wie die Daten verwendet und/oder weitergegeben werden: Wenn Sie Daten für einen bestimmten Zweck anfordern, aber auch für einen anderen Zweck nutzen, müssen Sie die Nutzer über beide Anwendungsfälle informieren.
- Sie müssen Nutzern eine Hilfedokumentation zur Verfügung stellen, in der erklärt wird, wie Nutzer ihre Daten verwalten und aus Ihrer App löschen können.

Sichere Datenverarbeitung

Sie müssen alle Nutzerdaten auf sichere Weise handhaben. Ergreifen Sie angemessene und geeignete Maßnahmen, um alle Anwendungen oder Systeme, die Health Connect nutzen, vor unbefugten oder unrechtmäßigen Zugriffen, Verwendungen, Zerstörungen, Verlusten, Änderungen oder Offenlegungen zu schützen.

Zu den empfohlenen Sicherheitsmaßnahmen zählen die Implementierung und Aufrechterhaltung eines Informationssicherheits-Managementsystems gemäß Standard ISO/IEC 27001. Darüber hinaus sollten Sie dafür sorgen, dass Ihre App oder Ihr Webdienst robust ist und keine der im Bericht „OWASP Top 10“ beschriebenen häufigen Schwachstellen aufweist.

Abhängig von der API, auf die zugegriffen wird, und der Anzahl der Nutzerberechtigungen oder Nutzer verlangen wir, dass Ihre App oder Ihr Dienst einer regelmäßigen Sicherheitsprüfung unterzogen wird und Ihnen von einer dazu bestimmten Drittpartei ein Prüfbericht ausgestellt wird, wenn Ihr Produkt Daten vom Gerät des Nutzers überträgt.

Weitere Informationen zu den Anforderungen für Apps, die mit Health Connect eine Verbindung herstellen, finden Sie in diesem Hilfeartikel.

VPNService

Der VpnService ist eine Basisklasse, die Sie in Ihren Apps erweitern können, um eigene VPN-Lösungen zu erstellen. Nur Apps, in denen der VpnService verwendet wird und deren Hauptfunktion VPN ist, können einen sicheren Tunnel auf Geräteebene zu einem Remote-Server erstellen. Ausnahmen sind Apps, die einen Remote-Server benötigen, um ihre Hauptfunktion ausführen zu können. Dazu zählen:

- Apps für Jugendschutzeinstellungen und Unternehmensverwaltung
- Apps zur Erfassung der App-Nutzung
- Apps zur Gerätesicherheit (z.B. Virenschutz, Mobilgeräteverwaltung, Firewall)
- Netzwerkbezogene Tools (z.B. Remote-Zugriff)
- Web-Browser
- Apps des Mobilfunkanbieters, bei denen VPN erforderlich ist, um Telefonie oder Konnektivitätsdienste bereitzustellen

Der VpnService darf für Folgendes nicht verwendet werden:

- Erfassen personenbezogener und sensibler Nutzerdaten ohne deutliche Offenlegung und Einwilligung

- Weiterleitung oder Manipulation des Nutzer-Traffics von anderen Apps auf einem Gerät zu Monetarisierungszwecken (z. B. Weiterleitung des Anzeigen-Traffics über ein anderes Land als das des Nutzers)

Entwickler von Apps, die den VpnService nutzen, müssen

- die Nutzung des VpnService im Google Play-Eintrag dokumentieren,
- die Daten vom Gerät zum Endpunkt des VPN-Tunnels verschlüsseln und
- sich an alle Programmrichtlinien für Entwickler einschließlich der Richtlinien zu Anzeigenbetrug, Berechtigungen und Malware halten.

Berechtigung „Exakter Alarm“

Es wird eine neue Berechtigung, USE_EXACT_ALARM, eingeführt, die Apps ab Android 13 (Ziel-API-Level 33) den Zugriff auf die exakte Alarmfunktion ermöglicht.

USE_EXACT_ALARM ist eine eingeschränkte Berechtigung und Entwickler dürfen diese Berechtigung nur in Apps deklarieren, wenn für deren Hauptfunktion ein exakter Alarm notwendig ist. Apps, für die diese eingeschränkte Berechtigung angefordert wird, werden überprüft, und diejenigen, die die Kriterien für akzeptable Anwendungsfälle nicht erfüllen, dürfen nicht auf Google Play veröffentlicht werden.

Akzeptable Anwendungsfälle zur Nutzung der Berechtigung „Exakter Alarm“

Sie dürfen die USE_EXACT_ALARM-Funktion nur dann verwenden, wenn für die für den Nutzer bestimmte Hauptfunktion Ihrer App zeitgenaue Aktionen erforderlich sind. Das trifft unter anderem auf folgende Fälle zu:

- Die App ist ein Wecker oder ein Timer.
- Die App ist ein Kalender, der Ereignisbenachrichtigungen anzeigt.

Wenn ein Anwendungsfall für die exakte Alarmfunktion vorliegt, der oben nicht genannt wurde, sollten Sie prüfen, ob Sie SCHEDULE_EXACT_ALARM als Alternative nutzen können.

Weitere Informationen zur exakten Alarmfunktion finden Sie in diesem Leitfaden für Entwickler.

Missbrauch von Geräten und Netzwerken

Apps, die das Gerät des Nutzers, andere Geräte oder Computer, Server, Netzwerke, APIs oder Dienste, etwa andere Apps auf dem Gerät, Google-Dienste oder das Netz eines autorisierten Mobilfunkanbieters, stören, unterbrechen, beschädigen oder in unerlaubter Weise darauf zugreifen, sind nicht zulässig.

Apps bei Google Play müssen den Kernanforderungen zur Systemoptimierung von Android entsprechen, die in den Qualitätsrichtlinien für Apps bei Google Play dokumentiert sind.

Eine App, die über Google Play vertrieben wurde, darf sich ausschließlich anhand des Updatemechanismus von Google Play modifizieren, ersetzen oder aktualisieren lassen. Außerdem darf die App keinen ausführbaren Code (z. B. DEX-, JAR- oder SO-Dateien) von einer anderen Quelle als Google Play herunterladen. Diese Einschränkung gilt nicht für Code, der in einer virtuellen Maschine oder einem Interpreter ausgeführt wird, bei denen indirekter Zugriff auf Android-APIs besteht, wie etwa bei JavaScript in einer Webansicht oder einem Browser.

Apps oder Drittanbietercode (z. B. SDKs) mit interpretierten Sprachen (JavaScript, Python, Lua etc.), die zur Laufzeit geladen werden und beispielsweise nicht mit der App verpackt sind, dürfen bzw. darf keine potenziellen Verstöße gegen Google Play-Richtlinien ermöglichen.

Code, mit dem Sicherheitslücken eingeführt oder ausgenutzt werden, ist nicht zulässig. Informieren Sie sich im Programm zur Verbesserung der App-Sicherheit über die aktuellen Sicherheitsprobleme, die Entwicklern gemeldet wurden.

Da Google Play eine sichere und respektvolle Plattform bleiben soll, haben wir Richtlinien entwickelt, in denen schädliche oder unangemessene Inhalte definiert und verboten werden.

- Apps, die andere Apps bei der Schaltung von Werbung blockieren oder stören
- Schummel-Apps, die den Spielverlauf anderer Apps beeinflussen
- Apps, die das Hacken von Diensten, Software oder Hardware oder das Umgehen von Sicherheitsvorkehrungen ermöglichen oder eine entsprechende Anleitung geben
- Apps, die auf Dienste oder APIs in einer Weise zugreifen oder diese nutzen, die gegen die Nutzungsbedingungen verstößt
- Apps, die nicht für die weiße Liste zugelassen sind und versuchen, die Verwaltung des Energieverbrauchs des Systems zu umgehen
- Apps, die Dritten Proxydienste zur Verfügung stellen – Proxydienste dürfen nur von Apps angeboten werden, in denen diese Funktion klar und deutlich den Hauptzweck für Nutzer darstellt
- Apps oder Drittanbietercode (z. B. SDKs), die ausführbaren Code wie DEX-Dateien oder nativen Code von einer anderen Quelle als Google Play herunterladen
- Apps, durch die ohne vorherige Zustimmung des Nutzers andere Apps auf einem Gerät installiert werden
- Apps, die die Verteilung oder Installation von schädlicher Software ermöglichen oder damit in Verbindung stehen
- Apps oder Drittanbietercode (z. B. SDKs), die bzw. der eine Webansicht mit hinzugefügter JavaScript-Schnittstelle enthalten bzw. enthält, über die nicht vertrauenswürdige Webinhalte (z. B. HTTP-URLs) oder nicht verifizierte URLs geladen werden, die aus nicht vertrauenswürdigen Quellen stammen. Nicht vertrauenswürdige Quellen sind z. B. URLs, die durch nicht vertrauenswürdige Intents aufgerufen werden.

Anforderungen für Flag Secure

FLAG_SECURE ist ein Anzeige-Flag, das im Code einer App deklariert wird, um anzugeben, dass die Benutzeroberfläche sensible Daten enthält, die nur auf einer sicheren Oberfläche und nur während der Verwendung der App angezeigt werden sollen. Dieses Flag soll verhindern, dass die Daten in Screenshots erscheinen oder auf nicht sicheren Displays angezeigt werden. Entwickler deklarieren dieses Flag, wenn der Inhalt der App nicht außerhalb der App oder des Geräts des Nutzers angezeigt oder anderweitig übertragen werden soll.

Aus Sicherheits- und Datenschutzgründen müssen alle auf Google Play bereitgestellten Apps die FLAG_SECURE-Deklaration anderer Apps berücksichtigen. Das bedeutet, dass Apps keine Möglichkeiten zur Umgehung der FLAG_SECURE-Einstellungen in anderen Apps erleichtern oder schaffen dürfen.

Apps, die als Bedienungshilfe zulässig sind, sind von dieser Anforderung ausgenommen, solange sie keine durch FLAG_SECURE geschützten Inhalte speichern, übertragen oder im Cache speichern, sodass außerhalb des Geräts des Nutzers auf diese zugegriffen werden kann.

Irreführendes Verhalten

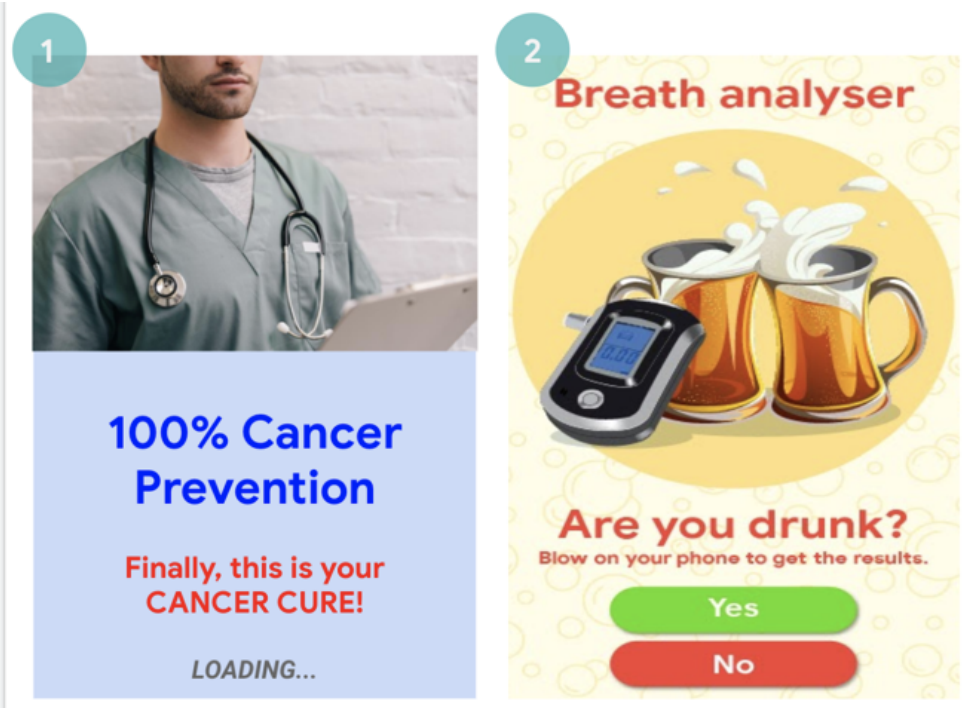
Apps, mit denen Nutzer getäuscht werden sollen oder die unlauteres Verhalten ermöglichen, sind nicht zulässig. Dazu gehören unter anderem Apps, die keine Funktion haben. Die Funktionalität von Apps muss in allen Teilen der Metadaten genau dargelegt, beschrieben und mit Bildern/Videos erläutert werden. Apps dürfen keine Funktionen oder Warnmeldungen des Betriebssystems oder anderer Apps nachahmen. Änderungen an Geräteeinstellungen dürfen nur mit Wissen und Zustimmung des Nutzers durchgeführt werden und müssen vom Nutzer wieder rückgängig gemacht werden können.

Irreführende Behauptungen

Apps, die falsche oder irreführende Informationen oder Behauptungen enthalten, sind nicht zulässig. Dies gilt auch für Beschreibungen, Titel, Symbole und Screenshots.

Da Google Play eine sichere und respektvolle Plattform bleiben soll, haben wir Richtlinien entwickelt, in denen schädliche oder unangemessene Inhalte definiert und verboten werden.

- Apps, deren Funktionalität falsch dargestellt oder nicht exakt und eindeutig beschrieben ist:
  - Eine App, die in der Beschreibung und den Screenshots als Rennspiel angegeben ist, tatsächlich aber ein Puzzlespiel mit dem Bild eines Autos ist
  - Eine App, die als Antiviren-App angepriesen wird, jedoch nur eine Textanleitung zur Entfernung von Viren enthält
- Apps mit vermeintlichen Funktionen, die sich nicht implementieren lassen (z. B. Apps zur Abwehr von Insekten), auch wenn sie als Streich, Fake, Scherz usw. dargestellt werden
- Apps, die nicht korrekt kategorisiert wurden, einschließlich, aber nicht beschränkt auf die App-Bewertung oder App-Kategorie
- Nachweislich betrügerische oder falsche Inhalte, mit denen Wahlen manipuliert werden können
- Apps, von denen fälschlicherweise behauptet wird, dass sie im Zusammenhang mit einer staatlichen Stelle stehen, oder staatliche Dienstleistungen anbieten oder vereinfachen und dafür nicht ordnungsgemäß autorisiert wurden
- Apps, von denen fälschlicherweise behauptet wird, dass es sich um die offizielle App eines etablierten Unternehmens handelt. Titel wie „Offizielle Justin Bieber App“ sind ohne die erforderlichen Genehmigungen oder Rechte nicht zulässig.



(1) Diese App enthält irreführende medizinische oder gesundheitsbezogene Behauptungen (Krebs heilen).
(2) Diese App enthält angeblich Funktionen, die in Wirklichkeit nicht realisierbar sind (Nutzung des Smartphones als Alkoholtester).

Betrügerische Änderungen von Geräteeinstellungen

Apps, die ohne Wissen und Zustimmung des Nutzers Änderungen an den Geräteeinstellungen oder -funktionen außerhalb der App vornehmen, sind nicht zulässig. Dies betrifft unter anderem System- und Browsereinstellungen, Lesezeichen, Verknüpfungen, Symbole, Widgets sowie die Darstellung von Apps auf dem Startbildschirm.

Darüber hinaus ist Folgendes unzulässig:

- Apps, die Geräteeinstellungen oder -funktionen mit Zustimmung des Nutzers ändern, ohne dass diese Änderungen problemlos wieder rückgängig gemacht werden können
- Apps oder Anzeigen, die als Dienst für Dritte oder zu Werbezwecken Geräteeinstellungen oder -funktionen ändern
- Apps, die Nutzer zur Entfernung oder Deaktivierung von Apps Dritter oder zur Änderung von Geräteeinstellungen oder -funktionen verleiten
- Apps, die Nutzer zur Entfernung oder Deaktivierung von Apps Dritter oder zur Änderung von Geräteeinstellungen oder -funktionen ermutigen oder anregen, es sei denn, es handelt sich hierbei nachweislich um einen sicherheitsbezogenen Dienst

Unlauteres Verhalten ermöglichen

Apps, mit denen Nutzer andere täuschen können oder die betrügerische Funktionen enthalten, sind nicht zulässig, darunter Apps, mit denen Ausweise, Sozialversicherungsnummern, Reisepässe, Abschlusszeugnisse, Kreditkarten, Bankkonten und Führerscheine erstellt werden können bzw. die deren Erstellung ermöglichen. Die Funktionalität und/oder der Inhalt der Apps müssen genau dargelegt und durch Titel, Beschreibungen sowie Bilder/Videos erläutert werden. Außerdem müssen sie erwartungsgemäß funktionieren.

Zusätzliche App-Ressourcen (z. B. Assets in Spielen) dürfen nur heruntergeladen werden, wenn sie für die Verwendung der App durch den Nutzer erforderlich sind. Heruntergeladene Ressourcen müssen alle Google Play-Richtlinien erfüllen. Vor Beginn des Downloads muss der Nutzer gefragt und deutlich auf die Downloadgröße hingewiesen werden.

Auch Apps, die als „Streich“, „zu Unterhaltungszwecken“ oder ähnlichen Zwecken veröffentlicht werden, müssen unseren Richtlinien entsprechen.

Da Google Play eine sichere und respektvolle Plattform bleiben soll, haben wir Richtlinien entwickelt, in denen schädliche oder unangemessene Inhalte definiert und verboten werden.

- Apps, mit denen andere Apps oder Websites nachgeahmt werden, um Nutzer zur Offenlegung von personenbezogenen Daten oder Authentifizierungsinformationen zu verleiten
- Apps, die unbestätigte oder echte Telefonnummern, Kontakte, Adressen oder personenidentifizierbare Informationen von natürlichen Personen oder Rechtspersönlichkeiten enthalten, die keine entsprechende Einwilligung gegeben haben
- Apps mit unterschiedlichen Kernfunktionen je nach geografischem Standort, Geräteparametern oder anderen nutzerbezogenen Daten, wobei im Store-Eintrag nicht deutlich auf diese Unterschiede hingewiesen wird
- Apps, die von Version zu Version deutlich verändert werden, ohne den Nutzer zu benachrichtigen (z. B. über den Abschnitt Neue Funktionen) und ohne den Store-Eintrag zu aktualisieren
- Apps, die versuchen, das Verhalten während der Überprüfung zu ändern oder zu verschleiern
- Apps, die Downloads über ein Content Delivery Network (CDN) durchführen und bei denen Nutzer vor Beginn des Downloads weder gefragt noch über die Downloadgröße informiert werden

Manipulierte Medien

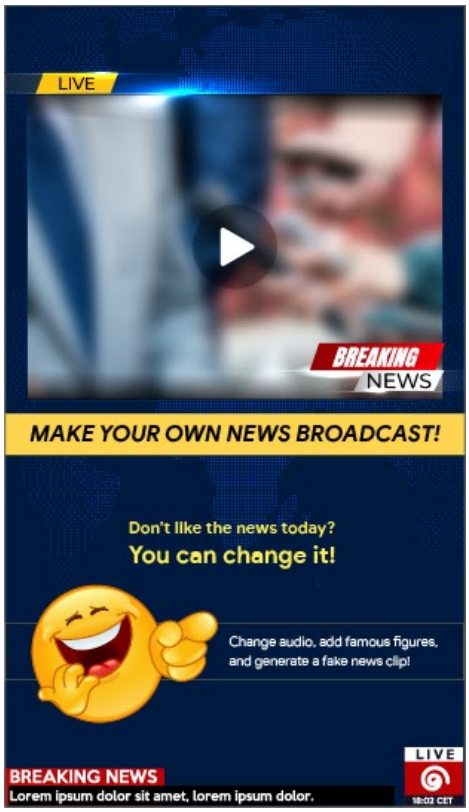
Apps, die zur Erstellung von falschen oder irreführenden Informationen oder Behauptungen in Form von Bildern, Videos und/oder Text dienen oder diese bewerben, sind nicht zulässig. Wir verbieten Apps, die nachweislich irreführende oder betrügerische Bilder, Videos und/oder Text bewerben oder verbreiten, die Schäden im Zusammenhang mit sensiblen Ereignissen, Politik, sozialen Themen oder anderen Angelegenheiten des öffentlichen Interesses verursachen können.

Apps, die Medien auf eine Weise manipulieren oder verändern, die über herkömmliche oder zu Redaktionszwecken akzeptable Veränderungen hinausgeht, müssen deutlich auf die bearbeiteten Medien hinweisen oder diese mit einem Wasserzeichen kennzeichnen, sollten die Änderungen für

Durchschnittsnutzer nicht klar ersichtlich sein. Es können Ausnahmen gewährt werden, sollte in diesem Zusammenhang ein öffentliches Interesse bestehen oder falls es sich offensichtlich um Satire oder eine Parodie handelt.

Da Google Play eine sichere und respektvolle Plattform bleiben soll, haben wir Richtlinien entwickelt, in denen schädliche oder unangemessene Inhalte definiert und verboten werden.

- Apps, die eine Person des öffentlichen Lebens zu Bildern oder Videos einer Demonstration zu einem politisch sensiblen Ereignis hinzufügen
- Apps, die Personen des öffentlichen Lebens oder Medien eines sensiblen Ereignisses verwenden, um die Funktionen zur Manipulation von Medien im Store-Eintrag der App zu bewerben
- Apps, die Medienclips verändern, um Nachrichtensendungen nachzuahmen



(1) Diese App bietet die Möglichkeit, Medienclips zu ändern, um eine Nachrichtensendung zu imitieren, und dem Clip bekannte Personen oder Personen des öffentlichen Lebens ohne Wasserzeichen hinzuzufügen.

Verhaltenstransparenz

Die Funktionalität Ihrer App sollte für Nutzer deutlich sein. Verwenden Sie keine versteckten, inaktiven oder undokumentierten Funktionen in Ihrer App. Techniken zur Umgehung von App-Rezensionen sind nicht zulässig. Mitunter bitten wir um zusätzliche Angaben zur App, damit wir die Nutzersicherheit, Systemintegrität und Einhaltung von Richtlinien sicherstellen können.

Falschdarstellung

Nicht zulässig sind Apps oder Entwicklerkonten,

- mit denen sich jemand als eine andere Person oder Organisation ausgibt oder deren Inhaber bzw. Hauptzweck falsch dargestellt oder verschleiert wird.
- die Nutzer durch koordinierte Aktivitäten täuschen. Dies schließt u. a. Apps oder Entwicklerkonten ein, die ihr Ursprungsland falsch darstellen oder geheim halten und sich mit ihren Inhalten an Nutzer eines anderen Landes richten.

- die mit anderen Apps, Websites, Entwicklern oder anderen Konten koordiniert werden, um die Entwickler- oder App-Identität oder andere wesentliche Details zu verschleiern oder falsch darzustellen. Dies gilt für alle Fälle, in denen sich die Inhalte auf politische und gesellschaftliche Themen sowie Belange von öffentlichem Interesse beziehen.

Ziel-API-Level-Richtlinie von Google Play

Wir möchten unseren Nutzern eine möglichst sichere Umgebung bieten. Aus diesem Grund sind folgende Ziel-API-Levels für **alle Apps** bei Google Play erforderlich:

Neue Apps und App-Updates MÜSSEN auf ein Android-API-Level ausgerichtet sein, das maximal ein Jahr hinter dem letzten größeren Android-Release zurückliegt. Neue Apps und App-Updates, die diese Anforderungen nicht erfüllen, können nicht in der Play Console eingereicht werden.

Bestehende Google Play-Apps, die nicht aktualisiert werden und die nicht auf ein API-Level ausgerichtet sind, das maximal zwei Jahre hinter dem letzten größeren Android-Release zurückliegt, sind nicht für neue Nutzer verfügbar, die Geräte mit neueren Android-Versionen verwenden. Nutzer, die die App zuvor über Google Play installiert haben, können sie weiterhin mit jeder von der App unterstützten Android-Version im Play Store finden, sie auf dem unterstützten Gerät neu installieren und dort nutzen.

Genauere Informationen dazu, wie Sie die Anforderungen bezüglich Ziel-API-Levels erfüllen, finden Sie im Migrationsleitfaden .

Die genauen Fristen und Ausnahmen finden Sie in diesem Hilfeartikel .

Anforderungen an SDKs

App-Entwickler verlassen sich oft auf Drittanbietercode (z. B. SDKs), um wichtige Funktionen und Dienste in ihren Apps anzubieten. Wenn Sie in Ihrer App ein SDK verwenden, sollten Sie zur Sicherheit Ihrer Nutzer beitragen und darauf achten, dass Ihre App bestmöglich vor Sicherheitslücken geschützt ist. In diesem Abschnitt erläutern wir, wie einige unserer bestehenden Anforderungen an Datenschutz und Sicherheit für die Verwendung von SDKs gelten und Entwickler dabei unterstützen sollen, SDKs auf sichere Weise in ihre Apps zu integrieren.

Beim Verwenden eines SDKs in Ihrer App sind Sie dafür verantwortlich, dass der Code und die Praktiken von Drittanbietern nicht dazu führen, dass Ihre App gegen die Google Play-Programmrichtlinien für Entwickler verstößt. Sie müssen sich darüber informieren, wie die SDKs in Ihrer App mit Nutzerdaten umgehen, welche Berechtigungen sie verwenden und welche Daten aus welchem Grund erhoben werden. Die Erhebung und Verarbeitung von Nutzerdaten durch ein SDK muss ebenso wie die Nutzung dieser Daten durch Ihre App richtlinienkonform sein.

Damit Ihre Nutzung von SDKs keinen Richtlinienverstoß darstellt, lesen Sie die folgenden vollständigen Richtlinien und beachten Sie außerdem die bestehenden Anforderungen im Hinblick auf SDKs.

Richtlinie zu Nutzerdaten

Sie müssen transparent machen, wie Sie mit Nutzerdaten umgehen (z. B. mit vom Nutzer bereitgestellten Informationen und Informationen, die über einen Nutzer erfasst werden, einschließlich Geräteinformationen). Das bedeutet: Sie müssen den Zugriff auf Nutzerdaten sowie deren Erhebung, Verwendung, Handhabung und Weitergabe durch Ihre App offenlegen und die Verwendung der Daten auf die offengelegten richtlinienkonformen Zwecke beschränken.

Wenn in Ihrer App Code von Drittanbietern enthalten ist, etwa ein SDK, müssen Sie sicherstellen, dass dieser in Ihrer App verwendete Code und die Praktiken des Drittanbieters im Hinblick auf Nutzerdaten aus Ihrer App den Google Play-Programmrichtlinien für Entwickler entsprechen, zu denen auch die Offenlegungspflichten gehören. So dürfen Ihre SDK-Anbieter beispielsweise keine personenbezogenen und vertraulichen Nutzerdaten aus Ihrer App verkaufen. Diese Anforderung gilt

unabhängig davon, ob Nutzerdaten weitergegeben werden, nachdem sie an einen Server gesendet wurden oder indem Drittanbietercode in Ihre App eingebettet wurde.

Personenbezogene und vertrauliche Nutzerdaten

- Sie müssen den appseitigen Zugriff auf personenbezogene und vertrauliche Daten sowie deren Erhebung, Verwendung und Weitergabe auf App- und Dienstfunktionen sowie richtlinienkonforme Zwecke beschränken, die vom Nutzer erwartet werden:
  - Apps, in denen personenbezogene und vertrauliche Nutzerdaten außerdem zur Bereitstellung von Werbung verwendet werden, müssen den Werberichtlinien von Google Play entsprechen.
- Alle personenbezogenen und vertraulichen Nutzerdaten müssen sicher verarbeitet und mit modernen Verschlüsselungsverfahren übertragen werden, z. B. über HTTPS.
- Fragen Sie, wenn möglich, Laufzeitberechtigungen an, bevor Sie über Android-Berechtigungsanfragen auf Daten zugreifen.

Verkauf von personenbezogenen und vertraulichen Nutzerdaten

Sie dürfen keine personenbezogenen und vertraulichen Nutzerdaten verkaufen.

- „Verkauf“ ist der Austausch personenbezogener und vertraulicher Nutzerdaten mit Dritten oder die Weitergabe an solche gegen Bezahlung.
  - Eine durch Nutzer initiierte Weitergabe personenbezogener und vertraulicher Nutzerdaten wird nicht als Verkauf betrachtet. Dazu gehört beispielsweise, wenn Nutzer eine Funktion einer App verwenden, um eine Datei an Dritte zu senden, oder wenn sie sich dafür entscheiden, eine App zu verwenden, die speziell für die Teilnahme an einer Forschungsstudie bestimmt ist.

Pflicht zur deutlichen Offenlegung und Einwilligung

In Fällen, in denen der appseitige Zugriff auf personenbezogene und vertrauliche Nutzerdaten sowie deren Erhebung, Verwendung oder Weitergabe nicht den angemessenen Erwartungen des Nutzers des betreffenden Produkts oder der betreffenden Funktion entsprechen, sind Sie zur deutlichen Offenlegung und Einwilligung gemäß der Richtlinie zu Nutzerdaten verpflichtet.

Wenn in Ihrer App Code von Drittanbietern enthalten ist, etwa ein SDK, das dazu dient, standardmäßig personenbezogene und vertrauliche Nutzerdaten zu erheben, müssen Sie innerhalb von zwei Wochen nach Erhalt einer Anfrage von Google Play (oder innerhalb des in der Google Play-Anfrage angegebenen Zeitraums, sofern dort ein anderer Zeitraum angegeben ist) ausreichend nachweisen, dass Ihre App die in dieser Richtlinie beschriebene Pflicht zur deutlichen Offenlegung und Einwilligung erfüllt, etwa im Hinblick auf Datenzugriff sowie Erhebung, Verwendung und Weitergabe von Daten durch Drittanbietercode.

Achten Sie darauf, dass Drittanbietercode (z. B. SDKs) nicht gegen die Richtlinie zu Nutzerdaten verstößt.

Weitere Informationen über die Pflicht zur deutlichen Offenlegung und Einwilligung finden Sie in diesem Hilfeartikel.

Beispiele für durch SDKs verursachte Verstöße

- Apps mit einem SDK, das personenbezogene und vertrauliche Nutzerdaten erhebt, das diese Daten aber nicht gemäß dieser Richtlinie zu Nutzerdaten, gemäß den Anforderungen an den Datenzugriff und die Handhabung der Daten (einschließlich des Verkaufsverbots) sowie gemäß der Pflicht zur deutlichen Offenlegung und Einwilligung verarbeitet.
- Apps mit einem SDK, das standardmäßig personenbezogene und vertrauliche Nutzerdaten erhebt und dabei gegen die Pflicht zur deutlichen Offenlegung und Einwilligung dieser Richtlinie verstößt.
- Apps mit einem SDK, das angibt, personenbezogene und vertrauliche Nutzerdaten nur zum Schutz vor Betrug und Missbrauch zu erheben, die erhobenen Daten jedoch auch zu Werbe- oder Analysezwecken an Dritte weitergibt.
- Apps mit einem SDK, das Informationen zu installierten Paketen von Nutzern überträgt, ohne dass die App die Pflicht zur deutlichen Offenlegung und/oder die Datenschutzrichtlinien einhält.
  - Weitere Informationen finden Sie in der Richtlinie zu unerwünschter Software für Mobilgeräte.

Weitere Anforderungen für den Zugriff auf personenbezogene und vertrauliche Daten

In der unten stehenden Tabelle werden weitere Anforderungen für bestimmte Aktivitäten erläutert.

Aktivität	Voraussetzung

Erhebung oder Verknüpfung gleichbleibender Geräte-IDs, z. B. IMEIs, IMSIs und SIM-Seriennummern	Gleichbleibende Geräte-IDs dürfen nicht mit anderen personenbezogenen und vertraulichen Nutzerdaten oder zurücksetzbaren Geräte-IDs verknüpft werden, mit folgenden Ausnahmen: • bei Anrufen über eine Telefonnummer, die mit einer SIM-Identität verknüpft ist, z. B. bei Anrufen über WLAN, wo die genutzte Nummer mit einem Mobilfunkanbieter-Konto verknüpft ist, und • bei Apps zur Verwaltung von Unternehmensgeräten im Geräte-Eigentümermodus. Diese Verwendungszwecke müssen für Nutzer entsprechend den Richtlinien zu Nutzerdaten deutlich offengelegt sein. In dieser Dokumentation finden Sie Informationen zu alternativen eindeutigen Kennzeichnungen. In der Werberichtlinie finden Sie zusätzliche Informationen zur Android-Werbe-ID.
Ausrichtung auf Kinder	Ihre App darf nur selbstzertifizierte SDKs enthalten, die für die Verwendung in auf Kinder ausgerichtete Dienste zugelassen sind. Die vollständigen Richtlinien und Anforderungen finden Sie unter Selbstzertifizierte Anzeigen-SDKs für familienfreundliche Inhalte.

Beispiele für durch SDKs verursachte Verstöße

- Apps mit einem SDK, das Android-IDs mit einem Standort verknüpft.
- Apps mit einem SDK, das zu Werbe- oder Analysezwecken AAIDs mit gleichbleibenden Geräte-IDs verknüpft.
- Apps mit einem SDK, das zu Analysezwecken AAIDs mit E-Mail-Adressen verknüpft.

Abschnitt zur Datensicherheit

Alle Entwickler müssen für jede App den Abschnitt zur Datensicherheit verständlich und wahrheitsgemäß ausfüllen. Dabei sind die Erhebung, Verwendung und Weitergabe von Nutzerdaten umfassend offenzulegen. Das gilt auch, wenn Daten über Bibliotheken oder SDKs von Drittanbietern, die Entwickler in ihren Apps verwenden, erhoben und verarbeitet werden. Der Entwickler ist für die Richtigkeit der Angaben im Abschnitt zur Datensicherheit und die laufende Aktualisierung dieser Informationen verantwortlich. Sofern relevant muss der Abschnitt den Offenlegungen in der Datenschutzerklärung der App entsprechen.

Weitere Informationen zum Ausfüllen des Abschnitts zur Datensicherheit finden Sie in diesem Hilfeartikel.

Die vollständige Richtlinie zu Nutzerdaten finden Sie hier.

Richtlinien zu Berechtigungen und APIs, die auf vertrauliche Informationen zugreifen

Anfragen für Berechtigungen und APIs, über die auf vertrauliche Informationen zugegriffen wird, sollten für die Nutzer Sinn ergeben. Sie dürfen lediglich Anfragen zu Berechtigungen und APIs stellen, über die auf vertrauliche Informationen zugegriffen wird, wenn diese Berechtigungen oder APIs zur Implementierung vorhandener Funktionen oder Dienste in Ihrer App erforderlich sind. Die Funktionen und Dienste müssen in Ihrem Google Play-Eintrag angegeben sein. Berechtigungen oder APIs, über die auf vertrauliche Informationen zugegriffen wird und die den Zugriff auf Nutzer- oder Gerätedaten für nicht offengelegte, nicht implementierte oder nicht zugelassene Funktionen oder Zwecke ermöglichen, dürfen nicht verwendet werden. Personenbezogene oder vertrauliche Daten, auf die über Berechtigungen oder APIs zugegriffen wird, dürfen niemals verkauft oder für einen Zweck weitergegeben werden, der den Verkauf möglich macht.

Die vollständigen Richtlinien zu Berechtigungen und APIs, über die auf vertrauliche Informationen zugegriffen wird, finden Sie hier.

Beispiele für durch SDKs verursachte Verstöße

- Ihre App verwendet ein SDK, das zu unzulässigen oder nicht angegebenen Zwecken den Zugriff auf die Standortermittlung im Hintergrund anfordert.
- Ihre App verwendet ein SDK, das über die Android-Berechtigung „read_phone_state“ ausgelesene IMEIs ohne Einwilligung durch den Nutzer überträgt.

Richtlinie zu Malware

Unsere Richtlinie zu Malware ist einfach: kein böswilliges Verhalten, also Malware, bei Android, im Google Play Store und auf Geräten von Nutzern. Mit diesem Grundsatz möchten wir Android zu einer möglichst sicheren Plattform für unsere Nutzer und ihre Geräte machen.

Malware ist jeglicher Code, der eine Gefahr für Nutzer, ihre Daten und ihre Geräte darstellt. Beispiele sind potenziell schädliche Apps (PSAs), Binärprogramme und Framework-Änderungen, wie z. B. Trojaner, Phishing- oder Spyware-Apps. Diese Kategorien werden von uns regelmäßig aktualisiert und ergänzt.

Die vollständige Richtlinie zu Malware finden Sie hier.

Beispiele für durch SDKs verursachte Verstöße

- Apps, die gegen das Berechtigungsmodell von Android verstoßen oder Anmeldedaten wie beispielsweise OAuth-Tokens von anderen Apps stehlen.
- Apps, die Funktionen missbrauchen, um zu verhindern, dass sie deinstalliert oder beendet werden können.
- Apps, die SELinux deaktivieren.
- Apps mit einem SDK, das gegen das Android-Berechtigungsmodell verstößt, indem es durch den Zugriff auf Gerätedaten zu unbekannten Zwecken Berechtigungen ausweitet.
- Apps mit einem SDK, das Nutzer auf betrügerische Weise dazu verleitet, Inhalte über die Abrechnung per Mobilfunkvertrag zu kaufen oder zu abonnieren.

Apps zur Rechteausweitung, die das Gerät ohne Zustimmung des Nutzers rooten, werden als Rooting-Apps eingestuft.

Richtlinie zu unerwünschter Software für Mobilgeräte

Transparenz und klare Offenlegung

Der gesamte Code sollte den Versprechen an den Nutzer entsprechen. Apps sollten alle kommunizierten Funktionen bieten. Apps dürfen Nutzer nicht verwirren.

Beispiele für Verstöße

- Werbebetrug
- Social Engineering

Nutzerdaten schützen

Der Zugriff, die Verwendung, die Erhebung und die Weitergabe personenbezogener und vertraulicher Nutzerdaten müssen klar und transparent sein. Die Verwendung von Nutzerdaten muss gegebenenfalls allen relevanten Richtlinien für Nutzerdaten entsprechen und es müssen alle Vorkehrungen zum Schutz der Daten getroffen werden.

Beispiele für Verstöße

- Datenerfassung (siehe Spyware)
- Missbrauch von eingeschränkten Berechtigungen

Die vollständige Richtlinie zu unerwünschter Software für Mobilgeräte finden Sie hier.

Richtlinie zum Missbrauch von Geräten und Netzwerken

Apps, die das Gerät des Nutzers, andere Geräte oder Computer, Server, Netzwerke, APIs oder Dienste, etwa andere Apps auf dem Gerät, Google-Dienste oder das Netz eines autorisierten Mobilfunkanbieters, stören, unterbrechen, beschädigen oder in unerlaubter Weise darauf zugreifen, sind nicht zulässig.

Apps oder Drittanbietercode (z. B. SDKs) mit interpretierten Sprachen (JavaScript, Python, Lua etc.), die zur Laufzeit geladen werden und beispielsweise nicht mit der App verpackt sind, dürfen bzw. darf keine potenziellen Verstöße gegen Google Play-Richtlinien ermöglichen.

Code, mit dem Sicherheitslücken eingeführt oder ausgenutzt werden, ist nicht zulässig. Informieren Sie sich im Programm zur Verbesserung der App-Sicherheit über die aktuellen Sicherheitsprobleme, die Entwicklern gemeldet wurden.

Die vollständige Richtlinie zum Missbrauch von Geräten und Netzwerken finden Sie hier.

Beispiele für durch SDKs verursachte Verstöße

- Apps, die Proxydienste für den Zugriff auf Inhalte Dritter zu Verfügung stellen – Proxydienste dürfen nur von Apps angeboten werden, in denen diese Funktion klar und deutlich den Hauptzweck für Nutzer darstellt.
- Apps mit einem SDK, das ausführbaren Code von einer anderen Quelle als Google Play herunterlädt, z. B. DEX-Dateien oder nativen Code.
- Apps mit einem SDK, das eine Webansicht mit hinzugefügter JavaScript-Schnittstelle enthält, über die nicht vertrauenswürdige Webinhalte (z. B. HTTP-URLs) oder nicht verifizierte URLs geladen werden, die aus nicht vertrauenswürdigen Quellen stammen. Nicht vertrauenswürdige Quellen sind z. B. URLs, die durch nicht vertrauenswürdige Intents aufgerufen werden.
- Apps mit einem SDK, das Code für die Aktualisierung des eigenen APKs enthält.
- Apps mit einem SDK, das Nutzer durch das Herunterladen von Dateien über eine unsichere Verbindung dem Risiko einer Sicherheitslücke aussetzt.
- Apps mit einem SDK, das Code für den Download oder die Installation von Apps aus anderen Quellen als Google Play enthält.

Richtlinie zu irreführendem Verhalten

Apps, mit denen Nutzer getäuscht werden sollen oder die unlauteres Verhalten ermöglichen, sind nicht zulässig. Dazu gehören unter anderem Apps, die keine Funktion haben. Die Funktionalität von Apps muss in allen Teilen der Metadaten genau dargelegt, beschrieben und mit Bildern/Videos erläutert werden. Apps dürfen keine Funktionen oder Warnmeldungen des Betriebssystems oder anderer Apps nachahmen. Änderungen an Geräteeinstellungen dürfen nur mit Wissen und Zustimmung des Nutzers durchgeführt werden und müssen vom Nutzer wieder rückgängig gemacht werden können.

Die vollständige Richtlinie zu irreführendem Verhalten finden Sie hier.

Verhaltenstransparenz

Die Funktionalität Ihrer App sollte für Nutzer deutlich sein. Verwenden Sie keine versteckten, inaktiven oder undokumentierten Funktionen Ihrer App. Techniken zur Umgehung von App-Rezensionen sind nicht zulässig. Von Apps können zusätzliche Angaben verlangt werden, um die Nutzersicherheit, Systemintegrität und Einhaltung von Richtlinien sicherzustellen.

Beispiel eines durch ein SDK verursachten Verstoßes

- Ihre App beinhaltet ein SDK, das Techniken zum Umgehen von App-Rezensionen verwendet.

Welche Verstöße gegen Google Play-Richtlinien für Entwickler werden häufig durch SDKs verursacht?

Damit Sie dafür sorgen können, dass jeglicher von Ihrer App verwendete Drittanbietercode den Programmrichtlinien für Entwickler von Google Play entspricht, lesen Sie bitte die folgenden Richtlinien:

- Richtlinie zu Nutzerdaten
- Berechtigungen und APIs, die auf vertrauliche Informationen zugreifen
- Richtlinie zum Missbrauch von Geräten und Netzwerken
- Malware
- Unerwünschte Software für Mobilgeräte
- Selbstzertifizierte Anzeigen-SDKs für familienfreundliche Inhalte
- Werberichtlinien
- Irreführendes Verhalten
- Google Play-Programmrichtlinien für Entwickler

Während gegen die genannten Richtlinien am häufigsten verstoßen wird, kann unsicherer SDK-Code auch zu Verstößen gegen andere Richtlinien führen. Lesen Sie alle Richtlinien vollständig und bleiben Sie über alle Änderungen auf dem Laufenden, da Sie als App-Entwickler die Verantwortung dafür tragen, dass Ihre SDKs App-Daten auf richtlinienkonforme Weise verarbeiten.

Weitere Informationen finden Sie in unserer Hilfe.

Malware

Unsere Richtlinie zu Malware ist einfach: kein böswilliges Verhalten, also Malware, bei Android, im Google Play Store und auf Geräten von Nutzern. Mit diesem Grundsatz möchten wir Android zu einer sicheren Plattform für unsere Nutzer und ihre Geräte machen.

Malware ist jeglicher Code, der eine Gefahr für Nutzer, ihre Daten und ihre Geräte darstellt. Beispiele sind potenziell schädliche Apps (PSA), Binärprogramme und Framework-Änderungen wie z. B. Trojaner, Phishing- oder Spyware-Apps. Diese Kategorien werden von uns regelmäßig aktualisiert und ergänzt.

Malware kann sich hinsichtlich ihrer Art und Funktion zwar unterscheiden, verfolgt aber in der Regel eines der folgenden Ziele:

- Die Integrität des Geräts kompromittieren
- Die Kontrolle über das Gerät übernehmen
- Ferngesteuerte Vorgänge ermöglichen, mit denen Angreifer auf das betroffene Gerät zugreifen, es verwenden oder es anderweitig missbrauchen können
- Personenbezogene Daten oder Anmeldedaten ohne ausreichende Offenlegung oder Zustimmung des Nutzers vom betroffenen Gerät aus versenden
- Spam oder Befehle über das betroffene Gerät verbreiten, um andere Geräte oder Netzwerke zu beeinträchtigen
- Den Nutzer betrügen

Apps, Binärprogramme oder Framework-Änderungen können potenziell schädlich sein und zu böswilligem Verhalten führen, selbst wenn sie nicht zu diesem Zweck erstellt wurden. Der Grund dafür ist, dass verschiedene Faktoren die Funktionsweise von Apps, Binärprogrammen und Framework-Änderungen beeinflussen können. Malware, die für ein Android-Gerät schädlich ist, muss deshalb nicht unbedingt für alle anderen Android-Geräte eine Gefahr darstellen. Schädliche Apps, die für ihr böswilliges Verhalten veraltete APIs verwenden, sind beispielsweise keine Bedrohung für Geräte, auf denen die neueste Version von Android installiert ist, können jedoch ein Risiko für Geräte mit alten Android-Versionen darstellen. Apps, Binärprogramme und Framework-Änderungen werden als Malware oder PSA eingestuft, wenn sie eine klare Gefahr für manche oder alle Android-Geräte und -Nutzer darstellen.

In den folgenden Malwarekategorien spiegelt sich unsere grundlegende Überzeugung wider, dass Nutzer verstehen sollten, wie ihr Gerät verwendet wird. Ziel ist es, eine sichere Umgebung zu fördern, die fortlaufende Innovation ermöglicht und Vertrauen bei Nutzern schafft.

Weitere Informationen finden Sie unter Google Play Protect .

Backdoors

Code, der die Ausführung von unerwünschten, potenziell schädlichen oder ferngesteuerten Vorgängen auf dem Gerät ermöglicht.

Dazu kann auch Verhalten zählen, dessen automatische Ausführung dazu führt, dass die App, das Binärprogramm oder die Framework-Änderung in eine der anderen Malwarekategorien fällt. Allgemein beschreibt der Begriff "Backdoor" einen potenziell schädlichen Vorgang auf einem Gerät, weshalb sich diese Kategorie nicht direkt mit anderen Kategorien wie dem Abrechnungsbetrug oder kommerzieller Spyware vergleichen lässt. Deshalb werden manche Backdoors unter Umständen von Google Play Protect als Sicherheitslücke eingestuft.

Abrechnungsbetrug

Code, mit dessen Hilfe Nutzern, durch absichtlich irreführende Praktiken, automatisch Kosten in Rechnung gestellt werden.

Betrug bei der Abrechnung über den Mobilfunkanbieter lässt sich in die Kategorien SMS-, Anruf- und Gebührenbetrug unterteilen.

SMS-Betrug
Code, durch den Nutzern, ohne ihre Zustimmung, das Senden von Premium-SMS in Rechnung gestellt oder versucht wird, SMS-Aktivitäten zu verschleiern. Das ist dann der Fall, wenn Offenlegungsvereinbarungen oder SMS des Mobilfunkanbieters versteckt werden, in denen der Nutzer über Gebühren informiert wird oder den Abschluss eines Abos bestätigen soll.

Für manche Codes wird zwar klar angegeben, wie sie sich in Bezug auf das Senden von SMS verhalten; das heißt aber noch nicht, dass SMS-Betrug dadurch generell ausgeschlossen werden kann. Beispiele sind das Verstecken oder Unlesbarmachen einzelner Abschnitte einer Offenlegungsvereinbarung oder das Unterdrücken von bestimmten SMS des Mobilfunkanbieters, in denen Nutzer über Gebühren informiert werden oder den Abschluss eines Abos bestätigen sollen.

Anrufbetrug
Code, durch den Nutzern Gebühren für Sonderrufnummern in Rechnung gestellt werden, obwohl sie keine Anrufe autorisiert haben.

Gebührenbetrug
Code, durch den Nutzer dazu verleitet werden, Inhalte zu abonnieren oder zu kaufen und sie über die Rechnung des Mobilfunkanbieters zu bezahlen.

Gebührenbetrug umfasst alle betrügerischen Abrechnungen mit Ausnahme von Premium-SMS und -Anrufen. Beispiele hierfür sind direkte Abrechnungen über den Mobilfunkanbieter, WAP-Betrug (Betrug über WLAN-Zugangspunkte) und Übertragungen, die über mobile Daten abgerechnet werden. WAP-Betrug zählt zu den häufigsten Arten des Gebührenbetrugs. Bei einem WAP-Betrug können Nutzer beispielsweise dazu verleitet werden, auf einem unbemerkt geladenen, transparenten WebView auf eine Schaltfläche zu klicken. Der Nutzer schließt dadurch ein Abo ab und die Bestätigungs-SMS oder -E-Mail wird in vielen Fällen gehackt, damit Nutzer die Finanztransaktion gar nicht erst bemerken.

Stalkerware

Code, der personenbezogene oder sensible Nutzerdaten eines Geräts erhebt und die Daten zu Überwachungszwecken an einen Dritten (Unternehmen oder eine andere Person) weiterleitet

Apps müssen eine angemessene deutliche Offenlegung enthalten und entsprechend der Richtlinie zu Nutzerdaten die Einwilligung der Nutzer einholen.

Richtlinien für Überwachungs-Apps

Nur Apps, die ausschließlich für die Überwachung einer anderen Person entworfen und vermarktet werden, beispielsweise für die Überwachung von Kindern durch Eltern oder Mitarbeitern durch Unternehmensführungen, sind als Überwachungs-Apps zulässig, sofern sie die unten beschriebenen Anforderungen vollständig erfüllen. Diese Apps dürfen jedoch nicht verwendet werden, um andere Personen (z. B. einen Partner) zu überwachen, auch nicht, wenn diese davon wissen und ihre Einwilligung gegeben haben, und unabhängig davon, ob ein dauerhaft sichtbarer Hinweis angezeigt wird. In diesen Apps muss das IsMonitoringTool-Metadatenflag in der Manifestdatei verwendet werden, um sie als Überwachungs-Apps zu kennzeichnen.

Überwachungs-Apps müssen diesen Anforderungen entsprechen:

- Die Apps dürfen nicht als Lösungen zur Spionage oder geheimen Überwachung angeboten werden.
- Die Apps dürfen eine solche Nachverfolgung nicht verheimlichen oder verschleiern oder Nutzer im Hinblick auf solche Funktionen täuschen.
- In den Apps muss dem Nutzer ein dauerhaft sichtbarer Hinweis eingeblendet werden, wenn sie ausgeführt wird, sowie ein Symbol zur eindeutigen Identifikation der App.
- In der Google Play Store-Beschreibung der App müssen Überwachungs- und Tracking-Funktionen offengelegt werden.
- Apps und ihre Einträge bei Google Play dürfen es Nutzern nicht ermöglichen, Funktionen zu aktivieren, die gegen diese Richtlinien verstoßen, oder auf solche Funktionen zuzugreifen, etwa durch einen Link zu einem nicht konformen APK außerhalb von Google Play.
- Apps müssen allen anwendbaren Gesetzen entsprechen. Für die Rechtmäßigkeit Ihrer App im jeweiligen Zielland sind allein Sie verantwortlich.

Im Hilfeartikel Verwendung des Flags „IsMonitoringTool“ finden Sie weitere Informationen.

Denial of Service (DoS)

Code, der dazu dient, ohne das Wissen des Nutzers einen DoS-Angriff (Denial of Service) durchzuführen, oder Code, der Teil eines dezentralen DoS-Angriffs auf andere Systeme oder Ressourcen ist.

Dies geschieht beispielsweise durch das Senden einer großen Anzahl von HTTP-Anfragen, um Remote-Server zu überlasten.

Schädliche Downloader

Code, der an sich zwar nicht schädlich ist, durch den aber weitere PSAs heruntergeladen werden.

In folgenden Fällen kann es sich um einen schädlichen Downloader handeln:

- Es besteht Grund zur Annahme, dass der Code zur Verbreitung von PSAs erstellt wurde und PSAs heruntergeladen hat bzw. dazu in der Lage ist, Apps herunterzuladen und zu installieren.
- Mindestens 5 % der von ihm heruntergeladenen Apps sind PSAs – der untere Grenzwert liegt hierfür bei 500 beobachteten App-Downloads (25 beobachtete PSA-Downloads).

Gängige Browser und Dateifreigabe-Apps sind keine schädlichen Downloader, solange Folgendes der Fall ist:

- Es werden keine Inhalte ohne Nutzerinteraktion heruntergeladen.
- Alle PSA-Downloads erfolgen mit der Zustimmung des Nutzers.

Bedrohung, die keine Gefahr für Android darstellt

Code, der Bedrohungen enthält, die keine Gefahr für Android darstellen.

Diese Apps stellen zwar kein Risiko für Android-Nutzer oder -Geräte dar, können aber für andere Plattformen schädlich sein.

Phishing

Code, der vorgibt, aus einer vertrauenswürdigen Quelle zu stammen, und Anmeldedaten für die Authentifizierung oder Zahlungsinformationen des Nutzers anfordert und die Daten an Dritte sendet. Auch Code, der Nutzerdaten abfängt, während diese übertragen werden, zählt zu dieser Kategorie.

Häufig sind Bankdaten, Kreditkartennummern und Anmeldedaten für soziale Netzwerke oder Spiele das Ziel von Phishing.

Missbrauch von erhöhten Berechtigungen

Code, der die Integrität des Systems dadurch gefährdet, dass er die App-Sandbox beeinträchtigt, Berechtigungen ausweitet oder den Zugriff auf sicherheitsrelevante Hauptfunktionen ändert oder deaktiviert.

Beispiele:

- Eine App, die gegen das Berechtigungsmodell von Android verstößt oder Anmeldedaten wie beispielsweise OAuth-Tokens von anderen Apps stiehlt
- Apps, die Funktionen missbrauchen, um zu verhindern, dass sie deinstalliert oder beendet werden können
- Eine App, die SELinux deaktiviert

Apps zur Rechteausweitung, die das Gerät ohne Zustimmung des Nutzers rooten, werden als Rooting-Apps eingestuft.

Ransomware (Erpressungstrojaner)

Code, der die teilweise oder komplette Kontrolle über ein Gerät oder Daten auf einem Gerät übernimmt und vom Nutzer eine Zahlung oder die Durchführung einer Aktion verlangt, um diese wieder freizugeben.

Manche Ransomware (Erpressungstrojaner) verschlüsselt die Daten auf dem Gerät und verlangt für die Entschlüsselung eine Zahlung. In einigen Fällen werden auch die Admin-Funktionen des Geräts verwendet, um zu verhindern, dass der Nutzer die Ransomware deinstallieren kann. Beispiele:

- Die Ransomware sperrt den Nutzer aus und verlangt im Austausch für die Kontrolle über das Gerät eine Zahlung.
- Die Daten auf dem Gerät werden verschlüsselt und die Ransomware behauptet, sie würde die Daten gegen eine Zahlung entschlüsseln.
- Die Ransomware nutzt Funktionen des Richtlinienmanagers, um die Deinstallation durch den Nutzer zu verhindern.

Code, der mit dem Gerät ausgeliefert wird und in erster Linie zur Unterstützung der Geräteverwaltung dient, wird möglicherweise nicht als Ransomware eingestuft. Dazu muss er die Anforderungen an die sichere Sperrung und Verwaltung sowie die Anforderungen zur deutlichen Offenlegung und zur Einholung der Nutzereinwilligung erfüllen.

Rooting

Code, der das Gerät rootet.

Rooting-Code ist nicht immer schädlich. Nicht schädliche Rooting-Apps informieren Nutzer vorab über den Root-Vorgang und führen keine potenziell schädlichen Aktionen aus, die unter andere PSA-Kategorien fallen.

Schädliche Rooting-Apps rooten das Gerät ohne das Wissen des Nutzers oder informieren Nutzer zwar vorab über den Root-Vorgang, führen jedoch Aktionen aus, die zu anderen PSA-Kategorien zählen.

Spam

Code, der unerwünschte Nachrichten an die Kontakte des Nutzers sendet oder das Gerät zum Versenden von E-Mail-Spam verwendet.

Spyware

Code, der personenbezogene Daten versendet, ohne den Nutzer ausreichend zu informieren oder seine Zustimmung einzuholen.

Beispielsweise wird die Übertragung folgender Daten als Spyware eingestuft, wenn dies ohne Offenlegung oder auf eine für den Nutzer unerwartete Weise geschieht:

- Kontaktliste
- Fotos oder andere Dateien von einer SD-Karte, die nicht zur App gehören
- Inhalte aus den E-Mails des Nutzers
- Anrufliste
- SMS-Liste
- Das Webprotokoll oder die Lesezeichen des Standardbrowsers
- Daten aus den "/data/"-Verzeichnissen anderer Apps

Verhaltensweisen, die als Ausspionieren des Nutzers betrachtet werden können, werden möglicherweise auch als Spyware eingestuft. Hierzu zählt beispielsweise das Aufzeichnen von Audio oder eingehenden Anrufen oder das Stehlen von App-Daten.

Trojaner

Code, der scheinbar ungefährlich ist – beispielsweise ein Spiel, das vorgibt, nur ein Spiel zu sein –, jedoch unerwünschte Aktionen durchführt.

Diese Klassifizierung wird oft in Kombination mit anderen PSA-Kategorien verwendet. Ein Trojaner hat beispielsweise eine harmlose und eine versteckte schädliche Komponente. Beispiel: Ein Spiel, das ohne das Wissen des Nutzers im Hintergrund Premium-SMS versendet.

Hinweis zu ungewöhnlichen Apps

Apps, die neuartig oder in ihrer Art eher selten sind, können als ungewöhnlich klassifiziert werden, wenn Google Play Protect nicht ausreichend Informationen hat, um sie als sicher einzustufen. Das bedeutet nicht, dass die App gefährlich ist, nur kann sie ohne weitere Überprüfung nicht als sicher eingestuft werden.

Hinweis zur Kategorie "Backdoor"

Ob Code unter die Malwarekategorie "Backdoor" fällt, hängt von seinem Verhalten ab. Code wird nur dann als Backdoor eingestuft, wenn seine automatische Ausführung ein Verhalten ermöglicht, durch das er unter eine der anderen Malwarekategorien fällt. Wenn eine App beispielsweise das dynamische Laden von Code erlaubt und so SMS extrahiert werden, wird die App als Backdoor-Malware eingestuft.

Wenn eine App jedoch die Ausführung von beliebigem Code erlaubt und kein Grund zur Annahme besteht, dass böswilliges Verhalten dahinter steckt, spricht man stattdessen von einer Sicherheitslücke, die der Entwickler mit einem Patch beheben muss.

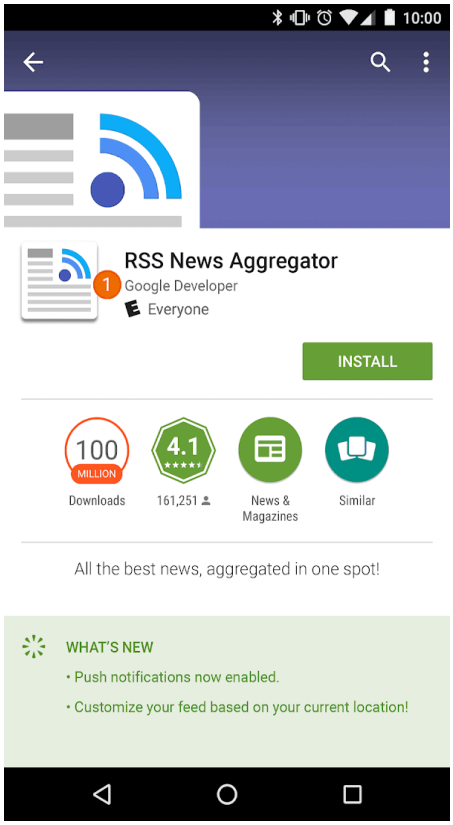
Identitätsdiebstahl

Apps, die Nutzer durch die Verwendung einer anderen Identität (z. B. die eines anderen Entwicklers, eines anderen Unternehmens oder einer anderen Rechtspersönlichkeit) oder Nachahmung einer anderen App in die Irre führen, sind nicht zulässig. Geben Sie nicht fälschlicherweise an, dass Ihre App mit jemandem in Verbindung steht oder von jemandem autorisiert wurde. Achten Sie darauf, dass Sie

keine App-Symbole, Beschreibungen, Titel oder In-App-Elemente verwenden, die Nutzer hinsichtlich der Beziehung Ihrer App zu jemand anderem oder einer anderen App in die Irre führen könnten.

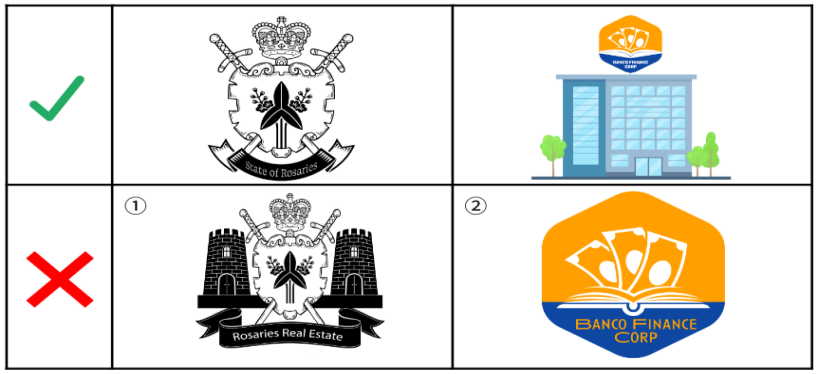
Da Google Play eine sichere und respektvolle Plattform bleiben soll, haben wir Richtlinien entwickelt, in denen schädliche oder unangemessene Inhalte definiert und verboten werden.

- Entwickler, die indirekt eine Beziehung zu einem anderen Unternehmen, einem Entwickler, einem Rechtssubjekt oder einer Organisation vortäuschen.



① Der für diese App angegebene Entwicklername suggeriert eine offizielle Verbindung zu Google, obwohl eine solche Verbindung nicht existiert.

- Apps, deren Symbole und Titel fälschlicherweise eine Beziehung zu einem anderen Unternehmen, einem Entwickler, einem Rechtssubjekt oder einer Organisation suggerieren.



① Für die App wird ein Staatssymbol verwendet, wodurch Nutzer glauben könnten, es handle sich um eine offizielle staatliche App.
② Für die App wurde das Logo eines Unternehmens kopiert, um zu suggerieren, dass es sich um eine offizielle App des Unternehmens handelt.

- App-Titel und -Symbole, die denen bereits vorhandener Produkte oder Dienste so ähnlich sind, dass Nutzer in die Irre geführt werden könnten.

① Das App-Symbol ist das Logo der Website einer beliebten Kryptowährung, um vorzutäuschen, es wäre die offizielle Website.
② Für die App wurden Figur und Titel einer berühmten Serie kopiert, wodurch Nutzer glauben könnten, es handle sich um eine offizielle App dieser Serie.

- Apps, von denen fälschlicherweise behauptet wird, dass es sich um die offizielle App eines etablierten Unternehmens handelt. Titel wie „Offizielle Justin Bieber App“ sind ohne die erforderlichen Genehmigungen oder Rechte nicht zulässig.
- Apps, die gegen die Android-Branding-Richtlinien verstoßen.

Mobile Unwanted Software

Unsere Überzeugung lautet: Der Nutzer steht an erster Stelle, alles Weitere folgt von selbst. In unseren Prinzipien in Bezug auf Software und der Richtlinie zu unerwünschter Software geben wir allgemeine Empfehlungen für Software, die eine optimale Nutzererfahrung bietet. Diese Richtlinie basiert auf der Google-Richtlinie zu unerwünschter Software. Sie enthält die Prinzipien für die Android-Plattform und den Google Play Store. Software, die gegen diese Prinzipien verstößt, beeinträchtigt die Nutzerfreundlichkeit, weshalb wir entsprechende Maßnahmen ergreifen, um unsere Nutzer davor zu schützen.

Wie in der Richtlinie zu unerwünschter Software angegeben, haben wir festgestellt, dass unerwünschte Software meistens eines oder mehrere derselben grundlegenden Merkmale aufweist:

- Sie ist irreführend und stellt ein Wertversprechen dar, das sie nicht hält.
- Sie versucht, den Nutzer durch Täuschung zur Installation zu bewegen, oder sie wird ungewollt in Verbindung mit einem anderen Programm installiert.
- Sie informiert den Nutzer nicht über alle ihre wesentlichen und wichtigen Funktionen.
- Sie hat unerwartete Auswirkungen auf das System des Nutzers.
- Sie sammelt oder überträgt private Informationen ohne Wissen des Nutzers.
- Sie erhebt oder überträgt private Informationen ohne sichere Verarbeitung (z. B. Übertragung über HTTPS).
- Sie ist mit anderen Programmen gebündelt, ohne dass auf ihre Existenz hingewiesen wird.

Auf Mobilgeräten besteht Software aus Code, der in Form einer App, Binärdatei, Framework-Änderung usw. vorliegt. Um Software zu vermeiden, die schädlich für die Softwareumgebung ist oder die Nutzererfahrung beeinträchtigt, ergreifen wir Maßnahmen gegen Code, der gegen diese Prinzipien verstößt.

Im Folgenden wird die Richtlinie zu unerwünschter Software erweitert, um ihre Anwendung auf Software für Mobilgeräte auszuweiten. Ebenso wie diese Richtlinie werden wir auch die Richtlinie zu unerwünschter Software für Mobilgeräte weiter optimieren, um neue Arten von Missbrauch zu beheben.

Transparenz und klare Offenlegung

Der gesamte Code sollte den Versprechen an den Nutzer entsprechen. Apps sollten alle kommunizierten Funktionen bieten. Apps dürfen Nutzer nicht verwirren.

- Funktionen und Ziele von Apps sollten klar kommuniziert werden.
- Erklären Sie dem Nutzer explizit und deutlich, welche Systemänderungen von der App vorgenommen werden. Bieten Sie Nutzern die Möglichkeit, alle wichtigen Installationsoptionen und -änderungen zu prüfen und zu genehmigen.
- Die Software darf den Status des Geräts des Nutzers nicht falsch darstellen. Dies kann unter anderem dann vorkommen, wenn sie den Eindruck vermittelt, dass sich das System in einem kritischen Sicherheitsstatus befindet oder mit Viren infiziert ist.
- Setzen Sie keine ungültigen Aktivitäten ein, die dazu dienen, den Anzeigen-Traffic und/oder Conversions zu steigern.
- Apps, für die eine andere Identität (z. B. der Name eines anderen Entwicklers oder Unternehmens) verwendet wird oder die eine andere App nachahmen, um Nutzer in die Irre zu führen, sind nicht zulässig. Behaupten Sie nicht, dass Ihre App mit Dritten in Verbindung steht oder von ihnen autorisiert wurde, wenn das nicht der Fall ist.

Beispiele für Verstöße:

- Werbebetrug
- Social Engineering

Nutzerdaten schützen

Der Zugriff, die Verwendung, die Erhebung und die Weitergabe personenbezogener und vertraulicher Nutzerdaten müssen klar und transparent sein. Die Verwendung von Nutzerdaten muss gegebenenfalls allen relevanten Richtlinien für Nutzerdaten entsprechen und es müssen alle Vorkehrungen zum Schutz der Daten getroffen werden.

- Bieten Sie Nutzern die Möglichkeit, der Erhebung ihrer Daten zuzustimmen, bevor Sie sie auf dem Gerät erheben und senden. Hierzu gehören Daten zu Drittanbieterkonten, E-Mail-Adresse, Telefonnummer, installierten Apps, Dateien, Speicherorten und andere personenbezogene und vertrauliche Daten, von denen der Nutzer nicht erwartet, dass sie erhoben werden.
- Persönliche und vertrauliche Nutzerdaten, die erhoben werden, sollten sicher behandelt werden, einschließlich der Übertragung mithilfe moderner Kryptografie (z. B. über HTTPS).
- Software, einschließlich mobiler Apps, darf nur personenbezogene und vertrauliche Nutzerdaten an Server übertragen, wenn diese mit der Funktionalität der App zusammenhängen.

Beispiele für Verstöße:

- Datenerhebung (siehe Spyware)
- Missbrauch von eingeschränkten Berechtigungen

Beispiele für Richtlinien zu Nutzerdaten:

- *Nutzerdatenrichtlinie für Google Mobile-Dienste-Anforderungen*
- Nutzerdatenrichtlinie für Google API-Dienste

Die mobile Nutzung nicht beeinträchtigen

Die Nutzung sollte unkompliziert und leicht verständlich sein und auf klaren Entscheidungen des Nutzers basieren. Dem Nutzer sollte ein klares Wertversprechen geboten werden und die beworbene oder gewünschte Nutzung sollte nicht beeinträchtigt werden.

- Schalten Sie keine Anzeigen, die Nutzern auf unerwartete Weise angezeigt werden, beispielsweise durch Verschlechterung oder Beeinträchtigung der Nutzerfreundlichkeit von Gerätefunktionen oder außerhalb der Umgebung der auslösenden App ohne entsprechende Einwilligung und ohne dass die Anzeigen leicht zu schließen und angemessen zuzuordnen sind.
- Apps dürfen andere Apps oder die Nutzerfreundlichkeit des Geräts nicht beeinträchtigen.
- Die Möglichkeit zur Deinstallation sollte gegebenenfalls klar erkennbar sein.
- Software für Mobilgeräte sollte keine Aufforderungen des Betriebssystems oder anderer Apps nachahmen. Unterdrücken Sie keine Benachrichtigungen von anderen Apps oder Betriebssystemen, insbesondere solche, die den Nutzer über Änderungen an seinem Betriebssystem informieren.

Beispiele für Verstöße:

- Störende Werbung
- Unbefugte Nutzung oder Imitation von Systemfunktionen

Schädliche Downloader

Code, der an sich zwar keine unerwünschte Software ist, durch den aber andere unerwünschte Software für Mobilgeräte heruntergeladen wird.

In folgenden Fällen kann es sich um einen schädlichen Downloader handeln:

- Es besteht Grund zur Annahme, dass der Code zur Verbreitung von unerwünschter Software für Mobilgeräte erstellt wurde und solche Software heruntergeladen hat oder dazu in der Lage ist, Apps herunterzuladen und zu installieren.
- Mindestens 5 % der vom Code heruntergeladenen Apps sind unerwünschte Software für Mobilgeräte – der untere Grenzwert liegt hierfür bei 500 beobachteten App-Downloads (25 beobachtete Downloads von unerwünschter Software für Mobilgeräte).

Gängige Browser und Dateifreigabe-Apps sind keine schädlichen Downloader, solange Folgendes der Fall ist:

- Es werden keine Inhalte ohne Nutzerinteraktion heruntergeladen.
- Alle Softwaredownloads erfolgen mit der Zustimmung des Nutzers.

Werbebetrug

Werbebetrug ist streng verboten. Anzeigeninteraktionen, die generiert werden, um einem Werbenetzwerk zu vorzutäuschen, dass Traffic aus echtem Nutzerinteresse stammt, sind Werbebetrug. Dabei handelt es sich um ungültige Zugriffe. Werbebetrug kann das Nebenprodukt sein, wenn Entwickler Anzeigen auf unzulässige Weise implementieren, z. B. ausgeblendete Anzeigen; Anzeigen, die automatisch angeklickt werden; Ändern von Informationen und anderweitiges Nutzen nicht-menschlicher Handlungen (Spider, Bots usw.) oder menschlicher Aktivitäten, um ungültigen Anzeigen-Traffic zu generieren. Ungültige Zugriffe und Werbebetrug sind schädlich für Werbetreibende, Entwickler und Nutzer und führen zu einem langfristigen Verlust des Vertrauens in das mobile Anzeigensystem.

Da Google Play eine sichere und respektvolle Plattform bleiben soll, haben wir Richtlinien entwickelt, in denen schädliche oder unangemessene Inhalte definiert und verboten werden.

- Apps, die Anzeigen rendern, die für den Nutzer nicht sichtbar sind

- Apps, die automatisch Klicks auf Anzeigen generieren, ohne dass der Nutzer dies beabsichtigt, oder entsprechenden Netzwerkverkehr erzeugen, um betrügerische Klick-Gutschriften zu erzeugen
- Apps, die gefälschte Klicks zur Installationsattribution senden, um für Installationen bezahlt zu werden, die nicht aus dem Netzwerk des Absenders stammen
- Apps, die Anzeigen einblenden, wenn sich der Nutzer nicht auf der App-Oberfläche befindet
- Apps, die das Anzeigeninventar falsch darstellen, z. B. eine App, die Werbenetzwerken mitteilt, dass sie auf einem iOS-Gerät ausgeführt wird, obwohl sie tatsächlich auf einem Android-Gerät ausgeführt wird; Apps, die den Paketnamen, der monetarisiert wird, falsch darstellen

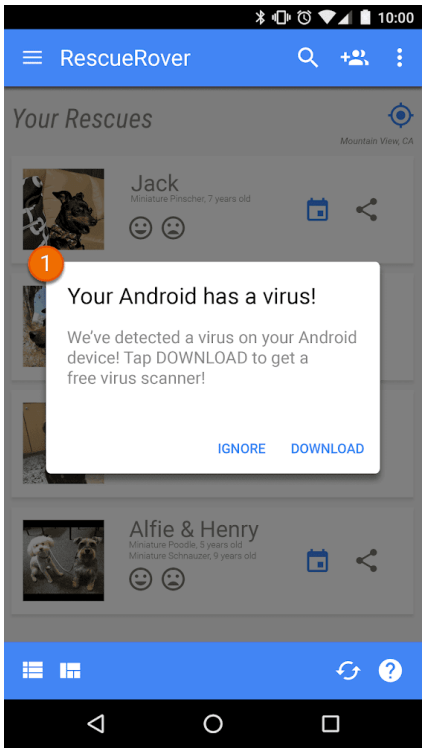
---

Unbefugte Nutzung oder Imitation von Systemfunktionen

Apps oder Anzeigen, die Systemfunktionen wie Benachrichtigungen oder Warnmeldungen nachahmen oder diese stören, sind nicht zulässig. Systembenachrichtigungen dürfen lediglich als integraler Bestandteil der App-Funktionen verwendet werden. So kann zum Beispiel die App einer Fluggesellschaft ihre Nutzer über Sonderangebote informieren oder in einem Spiel auf spielinterne Werbeaktionen hingewiesen werden.

Da Google Play eine sichere und respektvolle Plattform bleiben soll, haben wir Richtlinien entwickelt, in denen schädliche oder unangemessene Inhalte definiert und verboten werden.

- Apps oder Anzeigen, die im Rahmen einer Systembenachrichtigung oder Warnmeldung angeboten werden:



① Die in dieser App eingeblendete Systembenachrichtigung wird zur Schaltung von Werbung verwendet.

Weitere Beispiele in Verbindung mit Werbung finden Sie in den Werberichtlinien.

Social Engineering

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

Apps mit irreführender oder störender Werbung sind nicht zulässig. Die Werbeanzeigen dürfen nur innerhalb der jeweiligen App erscheinen. In Ihrer App geschaltete Werbeanzeigen werden als Teil Ihrer App angesehen und müssen daher sämtlichen Richtlinien entsprechen. Informationen über Richtlinien zu Glücksspielwerbung finden Sie hier.

Google Play unterstützt eine Reihe von Monetarisierungsstrategien, von denen Entwickler und Nutzer gleichermaßen profitieren, etwa das Anbieten von kostenpflichtigen Inhalten, In-App-Produkte, Abos und werbebasierte Modelle. Für eine optimale Nutzererfahrung ist die Einhaltung dieser Richtlinien unerlässlich.

Zahlungen

1. Entwickler, die den Download von Apps bei Google Play in Rechnung stellen, müssen für diese Transaktionen das Abrechnungssystem von Google Play als Zahlungsmethode verwenden.
2. Apps bei Google Play, bei denen eine Zahlung für den Zugang zu In-App-Funktionen oder -Diensten, einschließlich grundlegender App-Funktionen, digitaler Inhalte oder Waren (zusammenfassend „In-App-Käufe“) verlangt oder akzeptiert wird, müssen das Abrechnungssystem von Google Play für diese Transaktionen verwenden, sofern nicht Paragraf 3 oder Paragraf 8 Anwendung findet.

   Beispiele für App-Funktionen oder -Dienste, für die die Nutzung des Abrechnungssystems von Google Play erforderlich ist, sind unter anderem:

   - Artikel, z. B. virtuelle Währungen, zusätzliche Leben, zusätzliche Spieldauer, Add-on-Elemente, Figuren und Avatare
   - Abodienste, z. B. für Fitness, Spiele, Dating, Bildung, Musik, Videos, Upgrades von Diensten oder andere Inhalte
   - grundlegende App-Funktionen oder Inhalte wie eine App-Version ohne Werbung oder neue Funktionen, die in der kostenlosen Version nicht verfügbar sind
   - Cloud-Software und -Dienste, beispielsweise Datenspeicherdienste, Produktivitätssoftware für Unternehmen und Finanzverwaltungssoftware

3. Das Abrechnungssystem von Google Play darf in den folgenden Fällen nicht verwendet werden:
   a. Die Zahlung erfolgt hauptsächlich
      - für den Kauf oder Verleih von physischen Waren wie Lebensmitteln, Kleidung, Haushaltswaren, Elektronik;
      - für den Kauf physischer Dienstleistungen wie Beförderungsdienstleistungen, Reinigungsdiensten, Fluggebühren, Mitgliedschaften in Fitnessstudios, Lebensmittellieferungen, Eintrittskarten für Live-Veranstaltungen oder
      - als Überweisung zum Begleichen einer Kreditkartenabrechnung oder Rechnung eines Versorgungsunternehmens, beispielsweise Kabel- und Telekommunikationsdienstleisters.

   b. Zahlungen umfassen Peer-to-Peer-Zahlungen, Online-Auktionen und steuerbefreite Spenden.
   c. Die Zahlung erfolgt für Inhalte oder Dienste, die Onlineglücksspiele ermöglichen, wie im Abschnitt Glücksspiel-Apps der Richtlinie zu Glücksspielen, Spielen und Wettbewerben um echtes Geld beschrieben.
   d. Die Zahlung erfolgt für eine Produktkategorie, die gemäß den Inhaltsrichtlinien des Zahlungscenters von Google nicht akzeptiert wird.

      Hinweis: In einigen Märkten bieten wir Google Pay für Apps an, die physische Waren und/oder Dienstleistungen verkaufen. Weitere Informationen finden Sie auf der Google Pay-Entwicklerseite.

4. Außer unter den in Paragraf 3 und Paragraf 8 beschriebenen Bedingungen dürfen Apps Nutzer nicht zu einer anderen Zahlungsmethode als dem Abrechnungssystem von Google Play führen. Dieses Verbot umfasst unter anderem die Weiterleitung von Nutzern zu anderen Zahlungsmethoden über
   - den Eintrag einer App bei Google Play;
   - In-App-Werbung für käufliche Inhalte;
   - in Apps integrierte WebViews, Schaltflächen, Links, Werbebotschaften, Anzeigen oder andere Calls-to-Action und
   - In-App-Benutzeroberflächenabläufe, einschließlich Kontoerstellungs- oder Anmeldeabläufen, bei denen Nutzer von einer App zu einer anderen Zahlungsmethode als dem Abrechnungssystem von Google Play weitergeleitet werden.
5. Virtuelles In-App-Geld darf nur innerhalb der App oder des Spieltitels verwendet werden, in dem es ursprünglich erworben wurde.
6. Entwickler müssen Nutzer klar und genau über die Bedingungen und Preise ihrer App oder von zum Kauf angebotenen In-App-Funktionen oder Abos informieren. Die In-App-Preise müssen mit den Preisen übereinstimmen, die in der Google Play-Abrechnungsoberfläche angezeigt werden. Wenn sich Ihre Produktbeschreibung bei Google Play auf In-App-Funktionen bezieht, für die möglicherweise eine bestimmte oder zusätzliche Gebühr anfällt, müssen Nutzer in Ihrem App-Eintrag deutlich darüber informiert werden, dass für den Zugriff auf diese Funktionen eine Zahlung erforderlich ist.
7. Bei Apps und Spielen, in denen man über bestimmte Mechanismen durch einen Kauf zufällige virtuelle Elemente erhalten kann, einschließlich, aber nicht beschränkt auf sogenannte „Lootboxes“, muss die Chance, solche Elemente zu erhalten, vor dem Kauf und in enger zeitlicher Nähe zum Kauf klar offengelegt werden.
8. Sofern für die App keiner der in Paragraf 3 beschriebenen Fälle zutrifft, können Entwickler von Google Play-Apps für Mobilgeräte und Tablets Nutzern in Indien und/oder Südkorea zusätzlich zum Abrechnungssystem von Google Play ein alternatives Abrechnungssystem für Transaktionen anbieten, wenn bei diesen Apps von Nutzern eine Zahlung für den Zugang zu In-App-Käufen verlangt oder akzeptiert wird. Voraussetzung dafür ist das Ausfüllen des Erklärungsformulars über alternative Abrechnungssysteme (Indien, Südkorea) und die Zustimmung zu den darin enthaltenen zusätzlichen Bedingungen und Programmanforderungen.

Hinweis: In unserer Hilfe finden Sie Informationen zu Fristen und häufig gestellte Fragen bezüglich dieser Richtlinie.

Werbung

Für die Bewertung der Qualität Ihrer App berücksichtigen wir den Inhalt der Werbung, die Zielgruppe, die Nutzererfahrung, das Verhalten sowie die Sicherheit und den Datenschutz. Wir betrachten Werbung und die zugehörigen Angebote als Teil Ihrer App. Sie muss auch allen anderen Google Play-Richtlinien entsprechen. Wenn Sie eine App auf Google Play monetarisieren, die auf Kinder ausgerichtet ist, gelten zusätzliche Anforderungen an darin enthaltene Werbung.

Weitere Informationen zu unseren Richtlinien zu App-Werbung und Store-Einträgenund dazu, wie wir gegen irreführende Werbepraktiken vorgehen, finden Sie in diesem Artikel.

Werbeinhalt

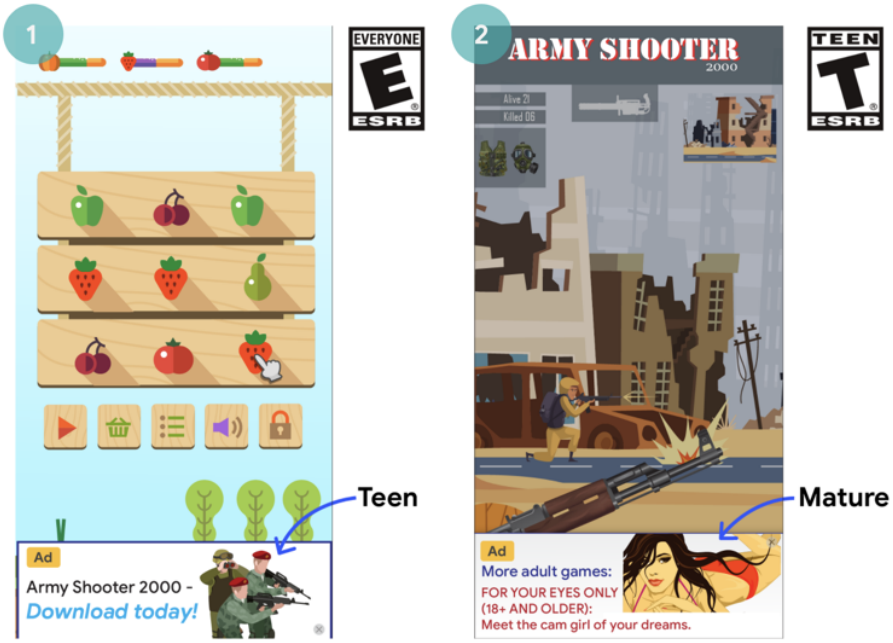
Werbung und die zugehörigen Angebote sind Teil Ihrer App und müssen unseren Richtlinien für eingeschränkte Inhalte entsprechen. Für Glücksspiel-Apps gelten zusätzliche Anforderungen.

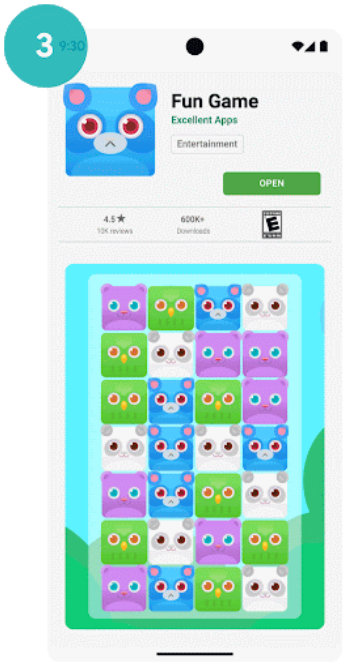
Unangemessene Werbung

Die Anzeigen und die damit verbundenen Angebote (z. B. Werbung für den Download einer anderen App), die in Ihrer App eingeblendet werden, müssen für die Altersfreigabe Ihrer App geeignet sein, auch wenn die Inhalte selbst ansonsten mit unseren Richtlinien übereinstimmen.

Da Google Play eine sichere und respektvolle Plattform bleiben soll, haben wir Richtlinien entwickelt, in denen schädliche oder unangemessene Inhalte definiert und verboten werden.

- Werbung, die für die Altersfreigabe der App unangemessen ist:





① Diese Werbung (Teenager) ist für die Altersfreigabe (Alle) dieser App unangemessen
② Diese Werbung (Erwachsene) ist für die Altersfreigabe (Teenager) dieser App unangemessen
③ Das Angebot der Werbung für den Download einer App mit nicht jugendfreien Inhalten ist für die Altersfreigabe der Spiele-App (Alle), in der die Anzeige eingeblendet wurde, unangemessen

Anforderungen an Werbung in familienfreundlichen Apps

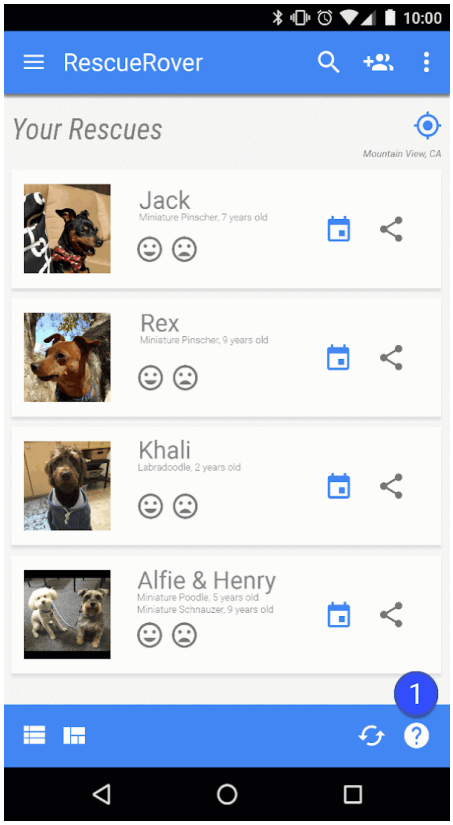
Wenn Sie eine App, die auf Kinder ausgerichtet ist, bei Google Play monetarisieren, muss sie die Anforderungen der Richtlinien zu Anzeigen und Monetarisierung in familienfreundlichen Apps erfüllen.

Irreführende Werbung

Werbeanzeigen dürfen die Benutzeroberfläche einer App-Funktion nicht simulieren oder nachahmen, etwa Benachrichtigungen oder Warnungen eines Betriebssystems. Es muss für Nutzer eindeutig erkennbar sein, über welche App die Werbeanzeige geschaltet wird.

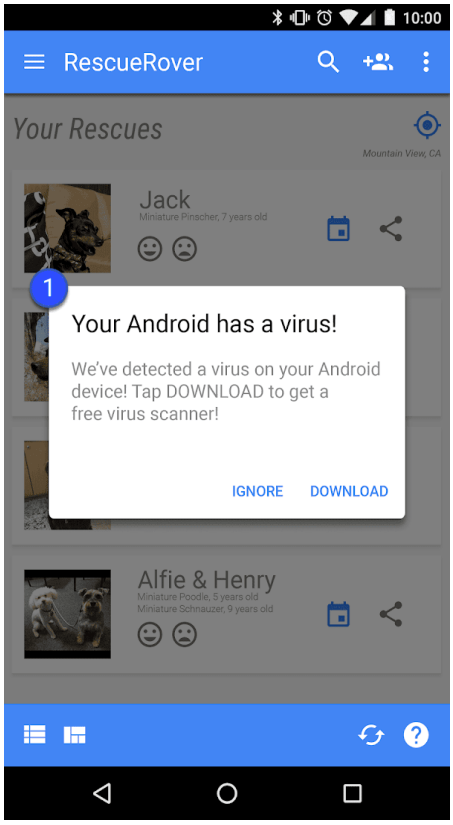
Da Google Play eine sichere und respektvolle Plattform bleiben soll, haben wir Richtlinien entwickelt, in denen schädliche oder unangemessene Inhalte definiert und verboten werden.

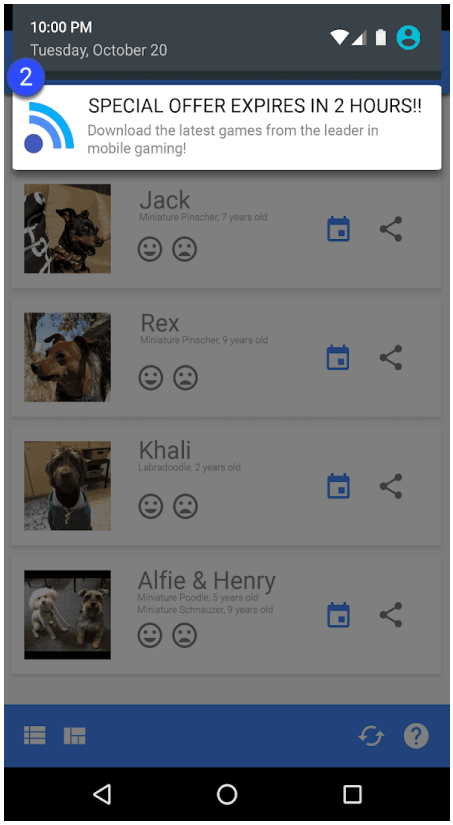
- Werbeanzeigen, die die Benutzeroberfläche einer App nachahmen:



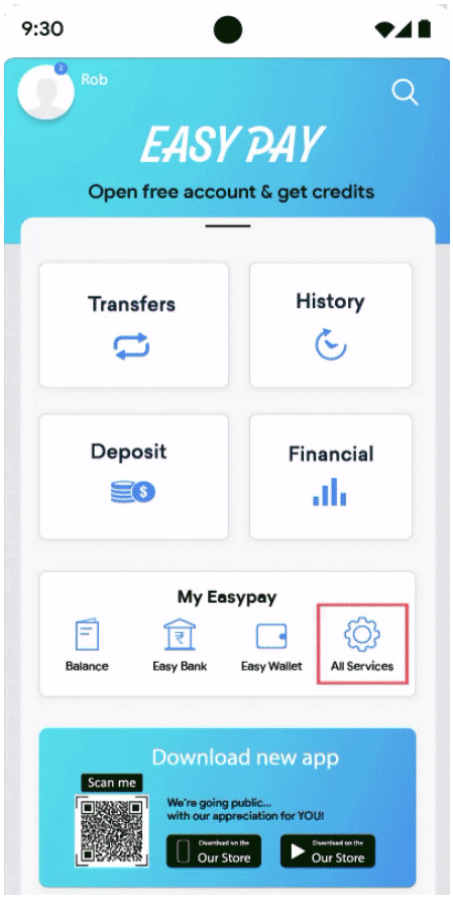
① Das Fragezeichensymbol in dieser App ist eine Werbeanzeige, die den Nutzer auf eine externe Landingpage weiterleitet.

- Werbeanzeigen, die Systembenachrichtigungen nachahmen:



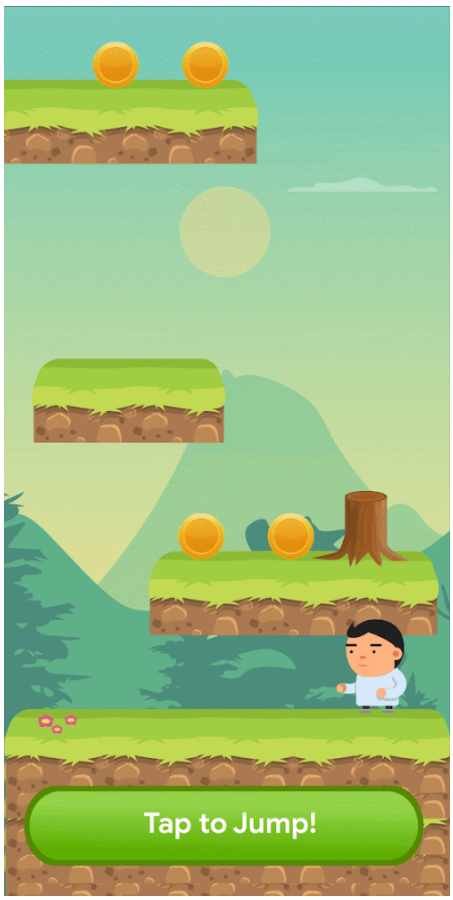


① ② Bei den Beispielen oben handelt es sich um Werbung, die verschiedene Systembenachrichtigungen nachahmt.



① Das Beispiel oben zeigt einen Funktionsbereich, der andere Funktionen nachahmt, Nutzer aber nur zu Werbung weiterleitet.

- Werbung, die plötzlich in einem Bereich erscheint, in dem Nutzer normalerweise auf In-App-Funktionen tippen:



① Hier wird Werbung eingeblendet, wenn der Nutzer auf die Schaltfläche zum Spielen tippt.

Störende Werbung

Als störende Werbung gilt Werbung, die Nutzern auf unerwartete Weise präsentiert wird und zu unbeabsichtigten Klicks oder einer Beeinträchtigung der Verwendung der Gerätefunktionen führen kann.

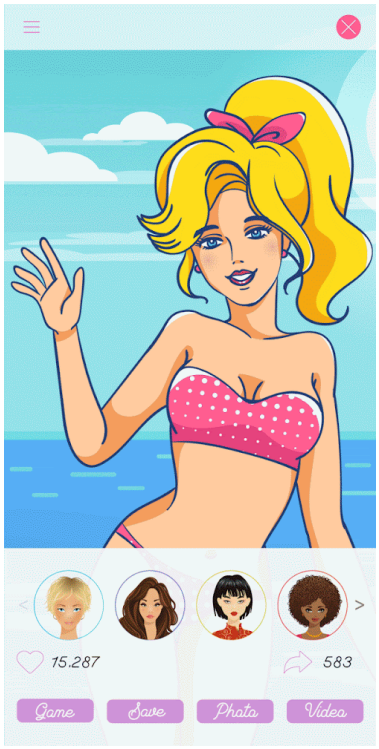
Nutzer dürfen nicht gezwungen werden, auf Werbung zu klicken oder personenbezogene Daten zu Werbezwecken zu senden, damit sie die App vollständig verwenden können. Werbung darf nur innerhalb der jeweiligen App präsentiert werden. Sie darf andere Apps und Anzeigen sowie die Nutzung des Geräts, einschließlich der System- und Gerätetasten sowie der Anschlüsse, nicht beeinträchtigen. Das gilt auch für Overlays, Companion-Anzeigen und Widget-Anzeigenblöcke. Wenn in Ihrer App Werbung geschaltet wird, die die normale Nutzung beeinträchtigt, muss sie sich einfach schließen lassen, ohne dass dem Nutzer daraus Nachteile entstehen.

Da Google Play eine sichere und respektvolle Plattform bleiben soll, haben wir Richtlinien entwickelt, in denen schädliche oder unangemessene Inhalte definiert und verboten werden.

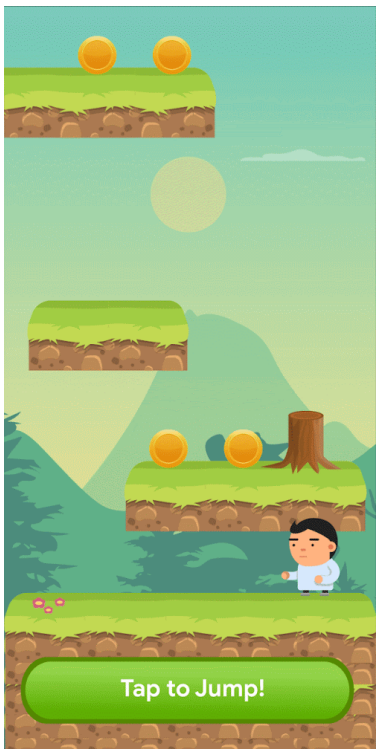
- Werbung, die den gesamten Bildschirm einnimmt oder die normale Nutzung beeinträchtigt und keine klar ersichtliche Möglichkeit zum Schließen bietet:

① Diese Werbung hat keine Schaltfläche zum Schließen.

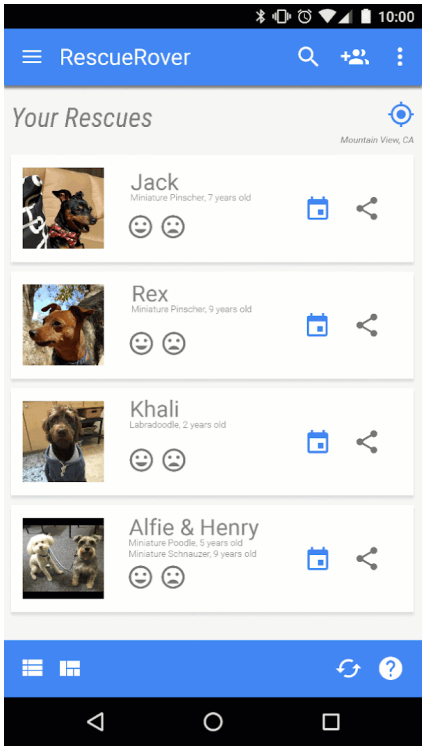
- Werbung, die Nutzer zum Anklicken zwingt, entweder durch eine falsche Schaltfläche zum Schließen oder dadurch, dass sie plötzlich in Bereichen der App erscheint, in denen Nutzer normalerweise auf andere Funktionen tippen:



① In dieser Werbung wird eine falsche Schaltfläche zum Schließen verwendet.

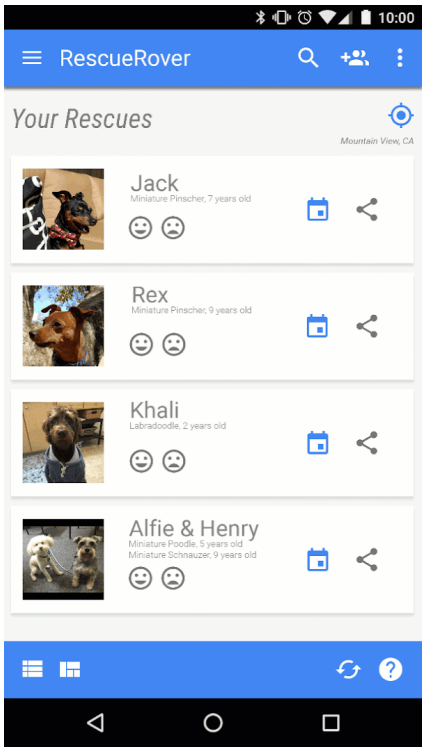


- Werbung, die außerhalb der jeweiligen App erscheint:



① Der Nutzer wechselt von der App zum Startbildschirm, wo plötzlich Werbung erscheint.

- Werbung, die durch die Startbildschirmtaste oder andere Funktionen ausgelöst wird, die explizit zum Verlassen der App vorgesehen sind:



① Der Nutzer versucht, die App zu verlassen und zum Startbildschirm zurückzukehren. Stattdessen wird der erwartete Ablauf aber durch Werbung unterbrochen.

Better Ads Experiences

Entwickler müssen die folgenden Anzeigenrichtlinien einhalten, um Nutzern bei der Verwendung von Google Play-Apps eine hohe Qualität zu bieten. Ihre Anzeigen dürfen nicht auf die folgenden für Nutzer unerwarteten Arten angezeigt werden:

- Vollbild-Interstitial-Anzeigen aller Formate (Video, GIF, statisch usw.), die unerwartet eingeblendet werden, in der Regel wenn der Nutzer etwas anderes tun möchte, sind nicht zulässig.
  - Anzeigen, die während des Spiels zu Beginn eines Levels oder zu Beginn eines Inhaltsabschnitts erscheinen, sind nicht zulässig.
  - Interstitial-Anzeigen mit Videovollbild, die vor dem Ladebildschirm einer App (Startbildschirm) eingeblendet werden, sind nicht zulässig.
- Vollbild-Interstitial-Anzeigen aller Formate, die sich nicht nach 15 Sekunden schließen lassen, sind nicht zulässig. Vollbild-Interstitials mit Opt-in oder Vollbild-Interstitials, die die Aktionen der Nutzer nicht unterbrechen (beispielsweise nach Anzeige des Spielstands in einer Gaming-App), dürfen länger als 15 Sekunden eingeblendet werden.

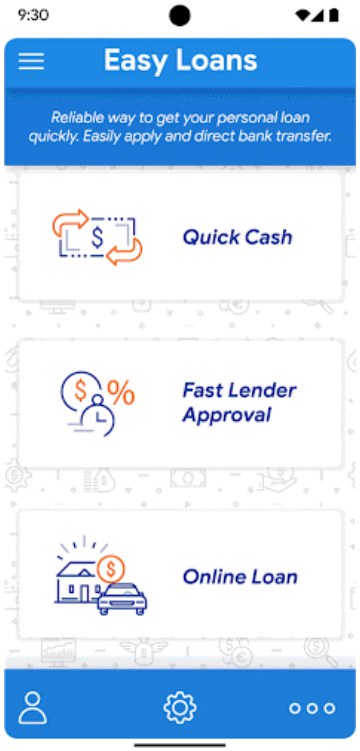
Diese Richtlinie gilt nicht für Anzeigen mit Prämie, der die Nutzer ausdrücklich zugestimmt haben (z. B. wenn sich Nutzer eine Anzeige ansehen und dafür ausdrücklich eine Prämie wie die Freischaltung einer bestimmten Spielfunktion oder eines bestimmten Inhalts erhalten). Diese Richtlinie gilt auch nicht für Monetarisierung und Werbung, die die normale Nutzung der App oder des Spiels nicht beeinträchtigt (z. B. Videoinhalte mit integrierten Anzeigen oder Banneranzeigen, die nicht im Vollbildmodus eingeblendet werden).

Damit orientieren wir uns an den Better Ads Experiences . Weitere Informationen zu den Better Ads Standards finden Sie auf der Website der Coalition of Better Ads .

Da Google Play eine sichere und respektvolle Plattform bleiben soll, haben wir Richtlinien entwickelt, in denen schädliche oder unangemessene Inhalte definiert und verboten werden.

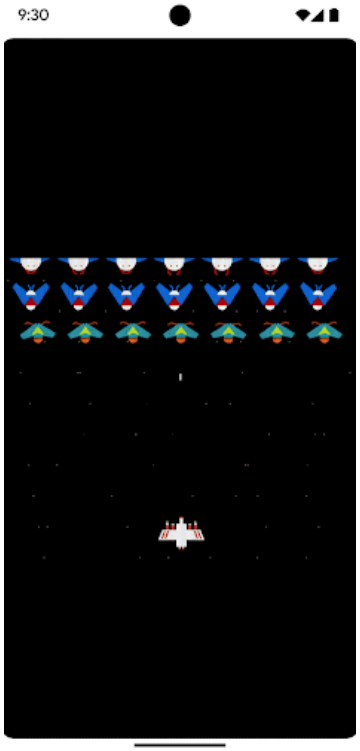
- Unerwartete Anzeigen, die während eines Spiels oder zu Beginn eines Inhaltsabschnitts erscheinen (z. B. nachdem ein Nutzer auf eine Schaltfläche geklickt hat und bevor die mit dem Klick auf die Schaltfläche beabsichtigte Aktion beginnt). Nutzer erwarten an dieser Stelle nicht, eine Anzeige zu sehen, da sie eigentlich ein Spiel beginnen oder mit Inhalten interagieren wollten.

① Eine unerwartete statische Anzeige wird während des Spiels zu Beginn eines Levels eingeblendet.



② Eine unerwartete Videoanzeige wird zu Beginn eines Inhaltsabschnitts eingeblendet.

- Eine Vollbildanzeige, die während des Spiels eingeblendet wird und nicht nach 15 Sekunden geschlossen werden kann



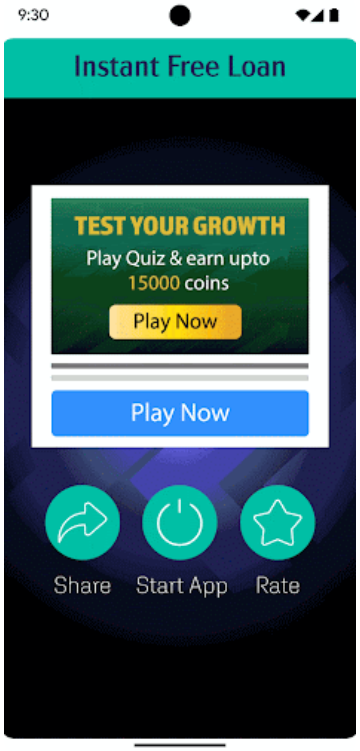
① Eine Interstitial-Anzeige wird während des Spiels eingeblendet und der Nutzer kann sie nicht nach 15 Sekunden überspringen.

Werbe-Apps

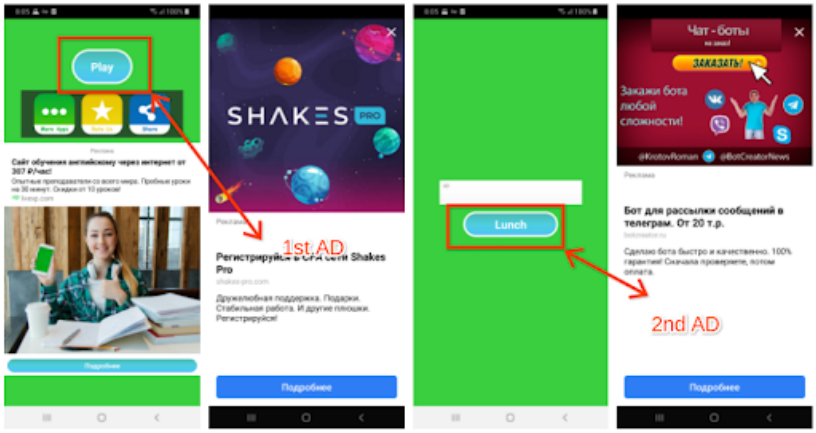
Apps, bei denen wiederholt Interstitial-Anzeigen eingeblendet und Nutzer so von der Interaktion mit einer App und dem Ausführen von Prozessen in der App abgelenkt werden, sind nicht zulässig.

Da Google Play eine sichere und respektvolle Plattform bleiben soll, haben wir Richtlinien entwickelt, in denen schädliche oder unangemessene Inhalte definiert und verboten werden.

- Apps, in denen Interstitial-Anzeigen nach einer Aktion des Nutzers (einschließlich, aber nicht beschränkt auf Klicken, Wischen usw.) aufeinanderfolgend platziert werden



① Auf der ersten In-App-Seite gibt es mehrere Schaltflächen, mit denen der Nutzer interagieren kann. Wenn der Nutzer auf **Start App** klickt, um die App zu verwenden, erscheint eine Interstitial-Anzeige in einem Pop-up-Fenster. Nachdem der Nutzer die Anzeige schließt, kehrt er zur App zurück und klickt auf **Service**, um den Service zu nutzen, aber eine weitere Interstitial-Anzeige wird eingeblendet.



② Auf der ersten Seite muss der Nutzer auf **Play** klicken, da es nur diese Schaltfläche gibt. Sobald der Nutzer darauf klickt, wird eine Interstitial-Anzeige eingeblendet. Nachdem er die Anzeige schließt, klickt der Nutzer auf **Launch**, da es keine weitere Schaltfläche gibt. Daraufhin wird eine weitere Interstitial-Anzeige eingeblendet.

Monetarisierung des Sperrbildschirms

Nur wenn Apps ausschließlich auf den Sperrbildschirm ausgerichtet sind, dürfen über sie Werbung oder Funktionen eingeführt werden, mit denen das gesperrte Display eines Geräts monetarisiert wird.

Werbebetrug

Werbebetrug ist streng verboten. Weitere Informationen finden Sie in unserer Richtlinie zu Werbebetrug.

Nutzung von Standortdaten zu Werbezwecken

Wenn Daten, die im Rahmen von Berechtigungen zur Ermittlung des Gerätestandorts eingeholt wurden, auch für die Schaltung von Werbung genutzt werden, müssen die Richtlinien für personenbezogene und vertrauliche Informationen eingehalten werden. Darüber hinaus gelten für solche Apps die folgenden Anforderungen:

- Der Nutzer muss eindeutig darauf hingewiesen werden, dass die im Rahmen der Berechtigung angeforderten Daten zum Gerätestandort zu Werbezwecken verwendet oder erhoben werden. Außerdem muss dies in der verbindlichen Datenschutzerklärung der App dokumentiert sein, einschließlich Links zu relevanten Datenschutzerklärungen von Werbenetzwerken, in denen die Nutzung von Standortdaten erläutert ist.
- In Einklang mit den Anforderungen bezüglich der Berechtigungen zur Standortermittlung dürfen diese nur angefordert werden, um vorhandene Funktionen oder Dienste in Ihrer App zu implementieren. Es ist nicht zulässig, Berechtigungen zur Ermittlung des Gerätestandorts ausschließlich zu Werbezwecken anzufordern.

Verwendung der Android-Werbe-ID

Mit Version 4.0 der Google Play-Dienste wurden neue APIs sowie eine ID eingeführt, die von Werbetreibenden und Anbietern von Analysediensten genutzt werden können. Die Bedingungen für die Nutzung dieser ID finden Sie unten.

- **Nutzung**: Die Android-Werbe-ID (Android Advertising Identifier, AAID) darf nur zu Werbezwecken sowie zur Nutzeranalyse verwendet werden. Der Status der Einstellung zur Deaktivierung interessenbezogener bzw. personalisierter Werbung muss bei jedem Zugriff auf die ID überprüft werden.
- **Verknüpfung mit personenidentifizierbaren Informationen oder sonstigen IDs**.
  - Verwendung für Werbung: Die Werbe-ID darf nicht zu Werbezwecken mit gleichbleibenden Geräte-IDs wie SSAID, MAC-Adresse oder IMEI verknüpft werden. Die Werbe-ID darf nur mit ausdrücklicher Zustimmung des Nutzers mit personenbezogenen Daten verknüpft werden.
  - Verwendung für Analysezwecke: Die Werbe-ID darf nur mit ausdrücklicher Zustimmung des Nutzers zu Analysezwecken mit personenidentifizierbaren Informationen oder gleichbleibenden Geräte-IDs wie SSAID, MAC-Adresse oder IMEI verknüpft werden. In der Richtlinie zu Nutzerdaten finden Sie zusätzliche Informationen zu gleichbleibenden Geräte-IDs.
- **Entscheidung der Nutzer respektieren**:
  - Nach Zurücksetzen der ID darf eine neue Werbe-ID nur mit ausdrücklicher Zustimmung des Nutzers mit einer vorherigen Werbe-ID oder daraus stammenden Daten verknüpft werden.
  - Sie müssen die vom Nutzer gewählte Einstellung zur Deaktivierung interessenbezogener bzw. personalisierter Werbung respektieren. Wenn ein Nutzer diese Einstellung aktiviert hat, dürfen Sie die Werbe-ID nicht zum Erstellen von Nutzerprofilen zu Werbezwecken oder zur Bereitstellung von personalisierten Anzeigen nutzen. Zulässig sind hingegen kontextbezogene Werbung, Frequency Capping, Conversion-Tracking, die Erstellung von Berichten sowie Sicherheits- und Betrugserkennung.
  - Auf neueren Geräten wird die Android-Werbe-ID entfernt, wenn sie von einem Nutzer gelöscht wird. Beim Versuch, auf die ID zuzugreifen, wird dann eine Folge von Nullen angezeigt. Ein Gerät ohne Werbe-ID darf nicht mit Daten verbunden werden, die mit einer früheren Werbe-ID verknüpft sind oder daraus stammen.
- **Transparenz gegenüber Nutzern**: Die Erfassung und Nutzung der Werbe-ID sowie die Verpflichtung zur Einhaltung dieser Bestimmungen muss den Nutzern in einer rechtlich angemessenen Benachrichtigung zum Datenschutz mitgeteilt werden. Weitere Informationen zu unseren Datenschutzstandards finden Sie in unserer Richtlinie zu Nutzerdaten .

- **Einhaltung der Nutzungsbedingungen**: Die Werbe-ID darf ausschließlich gemäß den Google Play-Programmrichtlinien für Entwickler verwendet werden. Dies gilt auch für sämtliche Parteien, an die Sie die ID im Rahmen Ihrer Geschäftstätigkeit weitergeben. In allen Apps, die bei Google Play hochgeladen oder veröffentlicht werden, muss zu Werbezwecken die Werbe-ID, sofern auf einem Gerät vorhanden, anstelle sonstiger Geräte-IDs verwendet werden.

Weitere Informationen finden Sie in unserer Richtlinie zu Nutzerdaten.

Abos

Als Entwickler dürfen Sie Nutzer hinsichtlich der im Abonnement für Ihre App enthaltenen Dienste oder Inhalte nicht täuschen. Achten Sie darauf, dass Sie Ihr Angebot bei allen In-App-Werbeaktionen und auf sämtlichen Startbildschirmen klar und deutlich kommunizieren. Apps, durch die Nutzer auf irreführende oder manipulative Weise zu Käufen verleitet werden, sind verboten. Hierzu zählen auch In-App-Käufe oder Abonnements.

Ihr Angebot muss jederzeit transparent sein. Dazu gehört auch, dass Sie Ihre Angebotsbedingungen ausdrücklich darlegen, beispielsweise die Kosten und den Abrechnungszeitraum für Ihr Abonnement sowie die Frage, ob ein Abonnement für die Nutzung der App erforderlich ist. Nutzer sollten nicht noch anderweitig recherchieren müssen, um an diese Informationen zu gelangen.

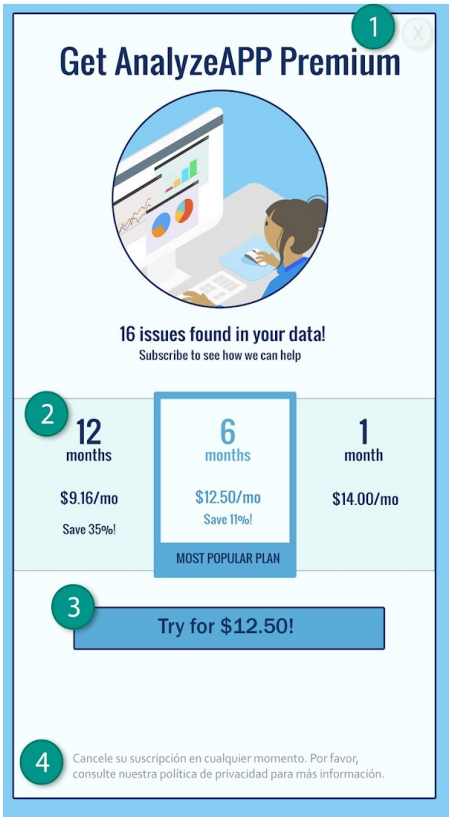
Abonnements müssen den Nutzern während ihrer gesamten Laufzeit einen dauerhaften oder wiederkehrenden Wert bieten. Sie dürfen nicht verwendet werden, um Nutzern letztendlich nur einen einmaligen Vorteil zu bieten, wie z. B. Produkte, die einmalige In-App-Guthaben/-Währungen oder einen nur einmal zu verwendenden Game Booster bringen. Ihr Abonnement kann zwar Anreize oder Werbeboni enthalten, diese müssen aber zusätzlich zu dem dauerhaften oder wiederkehrenden Wert angeboten werden, der während der gesamten Laufzeit des Abonnements vorhanden ist. Produkte, die keinen dauerhaften oder wiederkehrenden Wert bieten, müssen als In-App-Produkt anstelle eines Aboprodukts angeboten werden.

Sie dürfen einmalige Vorteile für Nutzer nicht als Abonnements tarnen oder falsch darstellen. Hierzu zählt auch die Umwandlung eines Abonnements in ein einmaliges Angebot (z. B. durch die Stornierung, Einstellung oder Verringerung des wiederkehrenden Werts), nachdem der Nutzer das Abonnement erworben hat.

Da Google Play eine sichere und respektvolle Plattform bleiben soll, haben wir Richtlinien entwickelt, in denen schädliche oder unangemessene Inhalte definiert und verboten werden.

- Monatsabos, bei denen Nutzer nicht darüber informiert werden, dass sie automatisch verlängert und monatlich in Rechnung gestellt werden.
- Jahresabos, bei denen offensiv mit den monatlichen Kosten geworben wird.
- Abopreise und -nutzungsbedingungen, die nicht vollständig lokalisiert sind.
- In-App-Werbeaktionen, bei denen nicht klar ersichtlich ist, dass Nutzer auch ohne Abonnement auf die Inhalte zugreifen können (sofern tatsächlich möglich).
- Artikelnamen, bei denen die Art des Abonnements nicht ersichtlich ist. Das ist beispielsweise der Fall, wenn von einer „kostenlosen Testversion“ oder von „Premium-Mitgliedschaft testen – 3 Tage kostenlos“ die Rede ist, obwohl dafür zukünftig regelmäßige Kosten anfallen.
- Mehrere Bildschirme im Kaufvorgang, die dazu führen, dass Nutzer versehentlich auf die Schaltfläche zum Abonnieren klicken.
- Abonnements, die keinen dauerhaften oder wiederkehrenden Wert bieten, wie z. B. das Angebot von 1.000 Edelsteinen für den ersten Monat des Abonnements und deren Verringerung auf 1 Edelstein in den Folgemonaten.
- Die Bedingung, dass ein Nutzer ein sich automatisch verlängerndes Abonnement abschließen muss, um einen einmaligen Vorteil zu erhalten, und die Kündigung des Abonnements nach dem Kauf, ohne dass der Nutzer dies wünscht.

Beispiel 1:



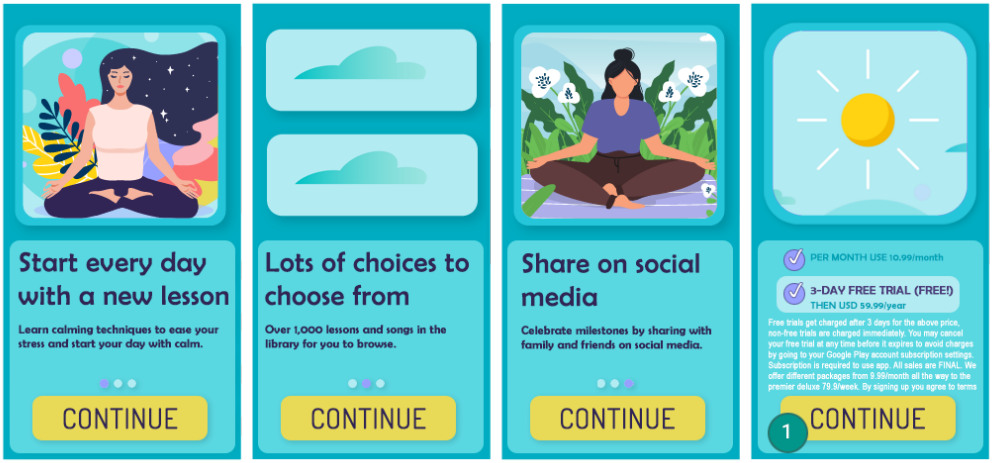
① Die Schaltfläche „Ablehnen“ ist nicht deutlich sichtbar, sodass Nutzer möglicherweise glauben, dass sie nur auf Funktionen zugreifen können, wenn sie ein Abonnement abschließen.

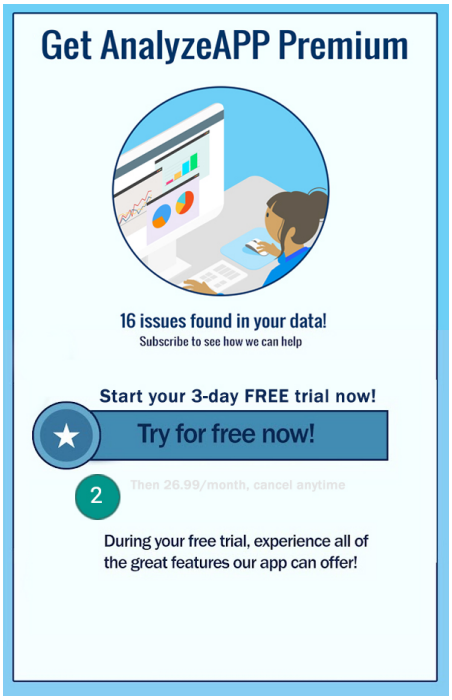
② Im Angebot werden nur die monatlichen Kosten angezeigt und Nutzer verstehen möglicherweise nicht, dass ihnen der Preis für sechs Monate berechnet wird, wenn sie ein Abo abschließen.

③ Im Angebot wird nur der Einführungspreis genannt und die Nutzer verstehen möglicherweise nicht, wie viel ihnen automatisch nach Ablauf der Einführungsphase in Rechnung gestellt wird.

④ Das Angebot sollte in derselben Sprache angezeigt werden wie die Nutzungsbedingungen, damit die Nutzer wirklich alle Aspekte des Angebots verstehen können.

Beispiel 2:





① Wiederholte Klicks im selben Schaltflächenbereich führen dazu, dass der Nutzer versehentlich auf die letzte Weiter-Schaltfläche klickt und sich damit für ein Abonnement anmeldet.

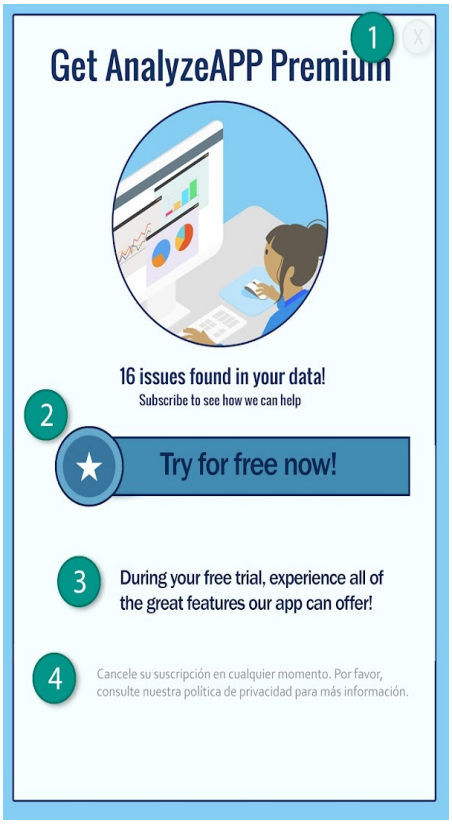
② Der Betrag, der den Nutzern am Ende des Testzeitraums in Rechnung gestellt wird, ist schlecht zu lesen, sodass der Nutzer denken könnte, dass das Angebot kostenlos sei.

Kostenlose Testversionen und Einstiegsangebote

Bevor ein Nutzer sich für eines Ihrer Abos anmeldet, gilt Folgendes: Sie müssen die Bedingungen Ihres Angebots, einschließlich der Dauer, des Preises und der Beschreibung der verfügbaren Inhalte oder Dienste, klar und deutlich beschreiben. Informieren Sie Ihre Nutzer, wie und wann eine kostenlose Testversion in ein kostenpflichtiges Abo umgewandelt wird und wie viel dieses kostet. Lassen Sie sie außerdem wissen, dass sie die Testversion kündigen können, wenn sie nicht möchten, dass sie in ein kostenpflichtiges Abo umgewandelt wird.

Da Google Play eine sichere und respektvolle Plattform bleiben soll, haben wir Richtlinien entwickelt, in denen schädliche oder unangemessene Inhalte definiert und verboten werden.

- Angebote, aus denen nicht eindeutig hervorgeht, wie lange die kostenlose Testversion verwendet werden kann oder wie lange der Einstiegspreis gilt.
- Angebote, aus denen nicht eindeutig hervorgeht, dass der Nutzer am Ende des Testzeitraums automatisch für ein kostenpflichtiges Abo angemeldet wird.
- Angebote, aus denen nicht eindeutig hervorgeht, dass Nutzer auch ohne Testversion auf die Inhalte zugreifen können (sofern möglich).
- Preise und Nutzungsbedingungen für Angebote, die nicht vollständig lokalisiert sind.



① Die Schaltfläche "Ablehnen" ist nicht deutlich sichtbar, sodass Nutzer möglicherweise glauben, dass sie nur auf Funktionen zugreifen können, wenn sie sich für die kostenlose Testversion registrieren.

② Das Angebot stellt die kostenlose Testversion in den Vordergrund, sodass Nutzern möglicherweise nicht klar ist, dass ihnen nach Ablauf des Testzeitraums eine Abogebühr in Rechnung gestellt wird.

③ Im Angebot wird kein Testzeitraum erwähnt, sodass Nutzer möglicherweise nicht wissen, wie lange sie kostenlos auf die Inhalte des Abos zugreifen können.

④ Das Angebot sollte in derselben Sprache angezeigt werden wie die Nutzungsbedingungen, damit die Nutzer wirklich alle Aspekte des Angebots verstehen können.

Abonnementverwaltung, Kündigung und Erstattungen

Wenn Sie in Ihrer App Abonnements verkaufen, müssen Sie deutlich offenlegen, wie ein Nutzer das Abonnement verwalten oder kündigen kann. Außerdem müssen Sie in Ihrer App eine Option einrichten, über die Nutzer ganz einfach online ihr Abonnement kündigen können. In den Kontoeinstellungen Ihrer App (oder einer entsprechenden Seite) können Sie diese Anforderung erfüllen, indem Sie Folgendes einfügen:

- Einen Link zum Abocenter von Google Play (für Apps, für die das Abrechnungssystem von Google Play verwendet wird) und/oder
- direkten Zugriff auf das Kündigungsverfahren.

Wenn ein Nutzer ein Abonnement kündigt, das er über das Abrechnungssystem von Google Play erworben hat, besteht gemäß unseren allgemeinen Richtlinien kein Anspruch auf Erstattung für den laufenden Abrechnungszeitraum. Er kann das Abonnement jedoch unabhängig vom Datum der Stornierung bis zum Ende dieses Zeitraums nutzen. Die Kündigung des Nutzers tritt mit Ablauf des laufenden Abrechnungszeitraums in Kraft.

Sie als Inhalts- oder Zugriffsanbieter können für Ihre Nutzer flexiblere Erstattungsrichtlinien festlegen. Dabei sind Sie verpflichtet, Ihre Nutzer zu informieren, wenn Sie Ihre Richtlinien zu Abonnements,

Kündigungen und Erstattungen ändern, und dafür zu sorgen, dass die Richtlinien nicht gegen geltendes Recht verstoßen.

Selbstzertifizierte Anzeigen-SDKs für familienfreundliche Inhalte

Wenn Sie in Ihrer App Werbeanzeigen ausliefern und die App nur für Kinder bestimmt ist, wie in der Richtlinie für familienfreundliche Inhalte beschrieben, müssen Sie selbstzertifizierte Anzeigen-SDK-Versionen verwenden, die den Google Play-Richtlinien sowie den Anforderungen an selbstzertifizierte Anzeigen-SDKs für familienfreundliche Inhalte entsprechen.

Ist die App sowohl für Kinder als auch für ältere Nutzer gedacht, müssen Sie gewährleisten, dass Werbeanzeigen, die Kindern präsentiert werden, ausschließlich von selbstzertifizierten Anzeigen-SDK-Versionen stammen (beispielsweise durch Maßnahmen zur neutralen Altersabfrage).

Beachten Sie, dass Sie dafür verantwortlich sind, dass jede in Ihrer App implementierte SDK-Version, auch selbstzertifizierte Anzeigen-SDK-Versionen, allen geltenden Richtlinien, lokalen Gesetzen und Bestimmungen entspricht. Google gibt keinerlei Gewährleistungen oder Garantien für die Richtigkeit der Angaben, die die Inhaber der Anzeigen-SDKs bei der Selbstzertifizierung machen.

Die Verwendung von selbstzertifizierten Anzeigen-SDKs für familienfreundliche Inhalte ist nur erforderlich, wenn Sie Anzeigen-SDKs nutzen, um Anzeigen für Kinder auszuliefern. Nachfolgend finden Sie Ausnahmen, die zulässig sind, ohne dass ein Anzeigen-SDK genutzt wird, das bei Google Play selbstzertifiziert wurde. Sie sind dennoch dafür verantwortlich, dass Anzeigeninhalte und Praktiken zur Datenerhebung der Richtlinie zu Nutzerdaten von Google Play sowie der Richtlinie für familienfreundliche Inhalte entsprechen. Zu den Ausnahmen gehören:

- Werbung in eigenen Properties, bei der Sie SDKs nutzen, um Cross-Promotion für Ihre Apps oder andere eigene Medien und Merchandise-Artikel zu verwalten
- Direct Deals mit Werbetreibenden, bei denen SDKs für die Inventarverwaltung verwendet werden

Anforderungen an selbstzertifizierte Anzeigen-SDKs für familienfreundliche Inhalte

- Legen Sie Definitionen für anstößige Anzeigeninhalte und unangemessenes Verhalten fest und verbieten Sie beides in den Nutzungsbedingungen bzw. Richtlinien des Anzeigen-SDK. Die Definitionen müssen den Google Play-Programmrichtlinien für Entwickler entsprechen.
- Entwickeln Sie eine Methode, mit der Sie Ihre Anzeigen danach einstufen können, ob sie sich für bestimmte Altersgruppen eignen. Dazu sollten in jedem Fall die Kategorien „Everyone“ (Jedes Alter) und „Mature“ (Nicht jugendfrei) gehören. Wenn für ein Anzeigen-SDK das Antragsformular unten ausgefüllt wurde, muss sich dessen Altersfreigabe-Methodik nach derjenigen richten, die Google für SDKs vorschreibt.
- Ermöglichen Sie es Publishern, entweder bei jeder Anfrage oder für jede App, eine auf Kinder ausgerichtete Anzeigenbereitstellung zu beantragen. Dabei müssen geltende Gesetze und Bestimmungen, wie der US Children's Online Privacy and Protection Act (COPPA) und die EU-Datenschutz-Grundverordnung (DSGVO), eingehalten werden. In Google Play müssen Anzeigen-SDKs personalisierte Werbeanzeigen, interessenbezogene Werbung und Remarketing bei allen Inhalten für Kinder deaktivieren.
- Ermöglichen Sie es Publishern, Anzeigenformate auszuwählen, die der Richtlinie zu Anzeigen und Monetarisierung in familienfreundlichen Apps von Google Play entsprechen und die Anforderungen an von Pädagogen empfohlene Apps erfüllen.
- Bei der Nutzung von Echtzeitgeboten zur Auslieferung von Werbeanzeigen an Kinder müssen die Creatives überprüft und Datenschutzrichtlinien von den Bietern beachtet werden.
- Stellen Sie genügend Informationen zur Verfügung (z. B. durch Einreichen einer Test-App oder im unten genannten Antragsformular), damit Google die Erfüllung aller Anforderungen an die Selbstzertifizierung seitens des Anzeigen-SDK bestätigen kann, und reagieren Sie zeitnah auf mögliche Nachfragen. Eventuell müssen Sie z. B. auch neue Versionen einreichen, damit geprüft

werden kann, ob die Anzeigen-SDK-Version allen Anforderungen an die Selbstzertifizierung entspricht, und eine Test-App einreichen.
- Bestätigen Sie per Selbstzertifizierung , dass alle neuen Versionen den aktuellen Google Play-Programmrichtlinien für Entwickler entsprechen, einschließlich der Richtlinie für familienfreundliche Inhalte.

Hinweis: Selbstzertifizierte Anzeigen-SDKs für familienfreundliche Inhalte müssen Ad Serving unterstützen, das allen relevanten Jugendschutzgesetzen und -bestimmungen entspricht, die für die Publisher gelten.

Weitere Informationen darüber, wie Sie Anzeigen-Creatives mit einem Wasserzeichen versehen und eine Test-App einreichen können, finden Sie hier .

Vermittlungsanforderungen für Anzeigenschaltungsplattformen bei der Auslieferung von Werbeanzeigen für Kinder:

- Nutzen Sie ausschließlich selbstzertifizierte Anzeigen-SDKs für familienfreundliche Inhalte oder implementieren Sie bestimmte Sicherheitsmaßnahmen, um zu gewährleisten, dass alle Werbeanzeigen, die durch Vermittlung ausgeliefert werden, diese Anforderungen erfüllen.
- Leiten Sie die erforderlichen Informationen an die Vermittlungsplattformen weiter, um diese über die Altersfreigabe für Anzeigeninhalte und etwaige Inhalte für Kinder in Kenntnis zu setzen.

Hier finden Entwickler eine Liste selbstzertifizierter Anzeigen-SDKs für familienfreundliche Inhalte , in der sie prüfen können, welche Versionen dieser SDKs für familienfreundliche Apps selbstzertifiziert sind.

Außerdem können Entwickler dieses Antragsformular an Anzeigen-SDK-Anbieter weiterleiten, die eine Selbstzertifizierung anstreben.

Store-Eintrag und Werbung

Die Bewerbung und die Sichtbarkeit Ihrer App wirken sich grundlegend auf die Qualität von Google Play aus. Vermeiden Sie daher Spameinträge, qualitativ minderwertige Werbung und Anstrengungen, die Sichtbarkeit Ihrer App bei Google Play künstlich zu verbessern.

App-Werbung

Apps, die direkt oder indirekt Werbepraktiken wie etwa Anzeigen nutzen, die den Nutzer in die Irre führen oder Nutzern bzw. Entwicklern schaden, sind nicht zulässig. Dies gilt auch für Apps, die von solchen Werbepraktiken profitieren. Werbepraktiken sind irreführend oder schädlich, wenn ihr Verhalten oder Inhalt gegen unsere Programmrichtlinien für Entwickler verstoßen.

Da Google Play eine sichere und respektvolle Plattform bleiben soll, haben wir Richtlinien entwickelt, in denen schädliche oder unangemessene Inhalte definiert und verboten werden.

- Irreführende Anzeigen auf Websites, in Apps oder an anderen Stellen, einschließlich nachgeahmter Systembenachrichtigungen und -warnungen
- Sexuell explizite Anzeigen , um Nutzer zum Google Play-Eintrag einer App weiterzuleiten, wo diese heruntergeladen werden kann
- Werbung oder Installationsmethoden, die zur Umleitung auf Google Play oder zum Download von Apps führen, ohne dass sich die Nutzer dessen bewusst sind
- Unerwünschte Werbung über SMS-Dienste
- Texte oder Bilder im App-Titel, Symbol oder Namen des Entwicklers, die auf die Leistung oder das Ranking im Play Store, Auszeichnungen oder Werbeaktionen hinweisen oder eine Verbindung mit vorhandenen Google Play-Programmen nahelegen

Sie müssen dafür sorgen, dass Werbenetzwerke, verbundene Unternehmen oder mit Ihrer App verknüpfte Anzeigen diese Richtlinien einhalten.

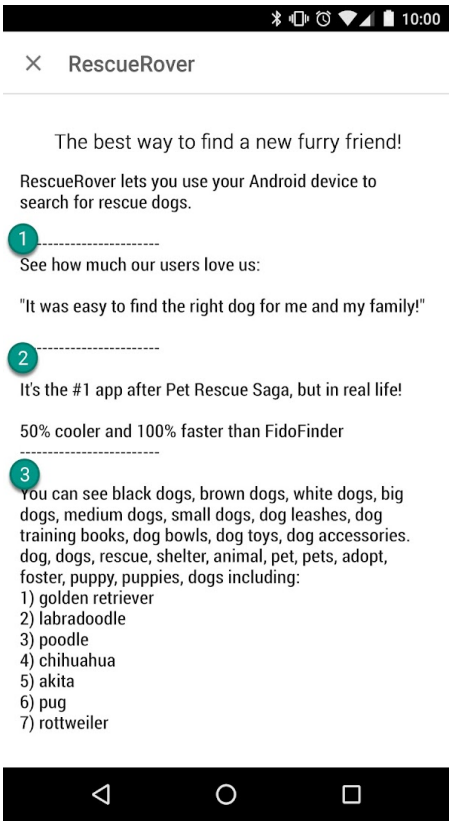
Metadaten

Nutzer müssen sich auf die Beschreibungen Ihrer App verlassen können, um deren Funktion und Zweck zu verstehen. Apps mit irreführenden, falsch formatierten, nicht aussagekräftigen, irrelevanten, übermäßigen oder unangemessenen Metadaten sind nicht zulässig. Dies schließt die Beschreibung, den Titel, das Symbol, Screenshots und Werbebilder der App sowie den Namen des Entwicklers ein. Entwickler müssen ihre App klar und deutlich beschreiben. Nicht zugeordnete oder anonyme Nutzerberichte sind in der Beschreibung der App nicht zulässig.

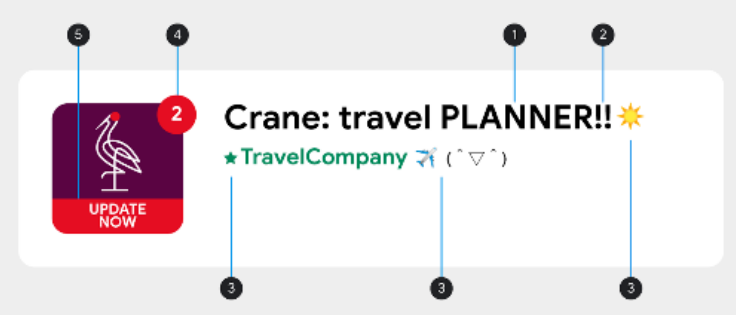
Der Titel und das Symbol Ihrer App sowie der Entwicklername sind besonders hilfreich für Nutzer, die Ihre App finden und mehr darüber erfahren möchten. Verwenden Sie keine Emojis oder Emoticons in diesen Metadatenelementen und reihen Sie keine Sonderzeichen aneinander. Verwenden Sie nicht ausschließlich GROSSBUCHSTABEN, es sei denn, es handelt sich um einen Markennamen. Irreführende Symbole in App-Symbolen sind nicht erlaubt, zum Beispiel Benachrichtigungspunkte für neue Nachrichten, wenn keine vorhanden sind, und Download-/Installationssymbole, wenn über die App keine Inhalte heruntergeladen werden können. Der Titel Ihrer App darf maximal 30 Zeichen lang sein. Es dürfen weder Texte noch Bilder im App-Titel, Symbol oder Namen des Entwicklers verwendet werden, die auf die Leistung oder das Ranking im Play Store, auf Informationen zum Preis oder zu Werbeaktionen hinweisen oder eine Verbindung mit vorhandenen Google Play-Programmen nahelegen.

Zusätzlich zu den hier genannten Anforderungen müssen Sie aufgrund bestimmter Google Play-Richtlinien für Entwickler unter Umständen weitere Metadaten angeben.

Da Google Play eine sichere und respektvolle Plattform bleiben soll, haben wir Richtlinien entwickelt, in denen schädliche oder unangemessene Inhalte definiert und verboten werden.

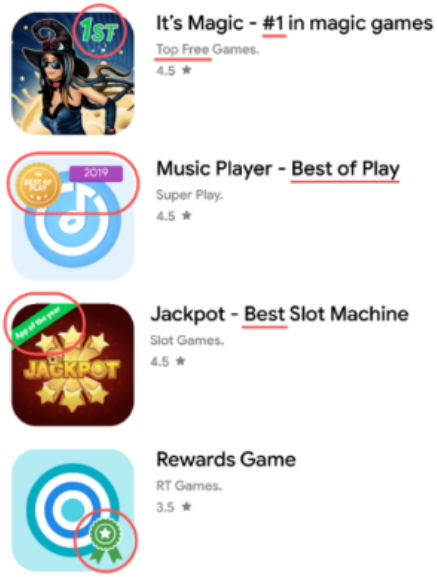


① Nicht zugeordnete oder anonyme Nutzerberichte
② Datenvergleich von Apps oder Marken
③ Aneinanderreihungen zusammenhangloser Wörter und vertikale/horizontale Wortlisten

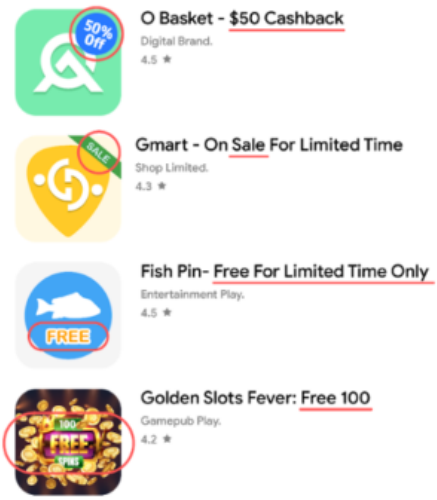


① GROSSSCHREIBUNG außerhalb des Markennamens
② Aneinanderreihungen von Sonderzeichen, die für die App irrelevant sind
③ Verwendung von Emojis, Emoticons (einschließlich Kaomojis) und Sonderzeichen
④ Irreführende Symbole
⑤ Irreführender Text

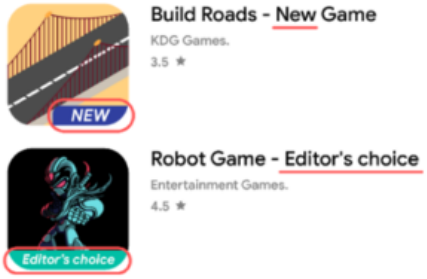
- Bilder oder Texte, die auf die Leistung oder das Ranking im Play Store hinweisen, wie „App des Jahres“, „Die Nummer 1“, „Bestes Spiel 20XX“, „Beliebt“, Symbole von Auszeichnungen etc.



- Bilder oder Texte, die den Preis oder andere Werbeinformationen enthalten, wie „10 % Rabatt“, „50 € Cashback“, „Nur für kurze Zeit kostenlos“ etc.



- Bilder oder Texte, die auf Google Play-Programme hinweisen, wie „Empfehlung der Redaktion“, „Neu“ etc.



Hier ein paar Beispiele für unangemessene Textinhalte, Bilder oder Videos in Ihrem Eintrag:

- Bilder oder Videos mit sexuell anzüglichen Inhalten Vermeiden Sie anzügliche Darstellungen von Brüsten, Gesäßen, Genitalien oder andere fetischisierte Körperdarstellungen bzw. Inhalte – egal, ob diese illustriert oder echt sind.
- Die Verwendung von anstößigen, vulgären oder anderen Ausdrücken, die für ein allgemeines Publikum im Store-Eintrag Ihrer App unangemessen sind.
- Darstellungen von drastischer Gewalt an auffälliger Stelle in App-Symbolen, Werbebildern oder Videos
- Darstellungen von gesetzeswidriger Verwendung von Drogen. Auch bildungsbezogene, dokumentarische, wissenschaftliche oder künstlerische Inhalte müssen im Store-Eintrag für alle Zielgruppen angemessen sein.

Hier ein paar Best Practices:

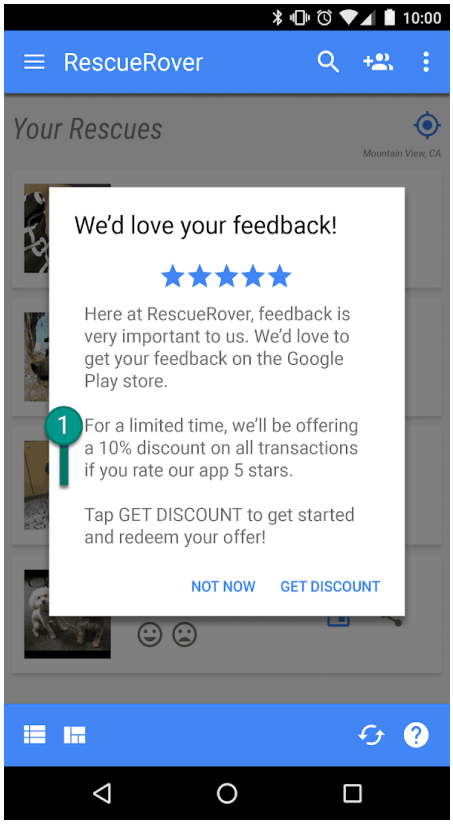
- Betonen Sie, was Ihre App einzigartig macht. Nennen Sie interessante und faszinierende Fakten zu Ihrer App, um Nutzern klarzumachen, was an Ihrer App so besonders ist.
- Achten Sie darauf, dass Titel und Beschreibung die Funktionen der App zutreffend wiedergeben.
- Vermeiden Sie irrelevante oder sich wiederholende Keywords oder Verweise.
- Die Beschreibung Ihrer App sollte kurz und klar sein. Eine kürzere Beschreibung lässt sich besonders auf Geräten mit kleinerem Bildschirm meist besser lesen. Übermäßige Länge, Details, falsche Formatierung oder Wiederholungen können zu einem Richtlinienverstoß führen.
- Beachten Sie, dass Ihr Eintrag für eine allgemeine Zielgruppe angemessen sein sollte. Vermeiden Sie in Ihrem Eintrag unangemessene Textinhalte, Bilder oder Videos und halten Sie die oben aufgeführten Richtlinien ein.

Bewertungen, Rezensionen und Installationen von Nutzern

Entwickler dürfen nicht versuchen, die Platzierung von Apps bei Google Play zu manipulieren. Unter anderem dürfen Produktbewertungen, Rezensionen oder die Zahl der Installationen nicht auf unzulässige Weise verbessert werden, etwa durch betrügerische oder durch Incentives motivierte Installationen, Rezensionen und Bewertungen. Die Hauptfunktion der App darf außerdem nicht darin bestehen, Nutzer zur Installation anderer Apps anzuregen.

Da Google Play eine sichere und respektvolle Plattform bleiben soll, haben wir Richtlinien entwickelt, in denen schädliche oder unangemessene Inhalte definiert und verboten werden.

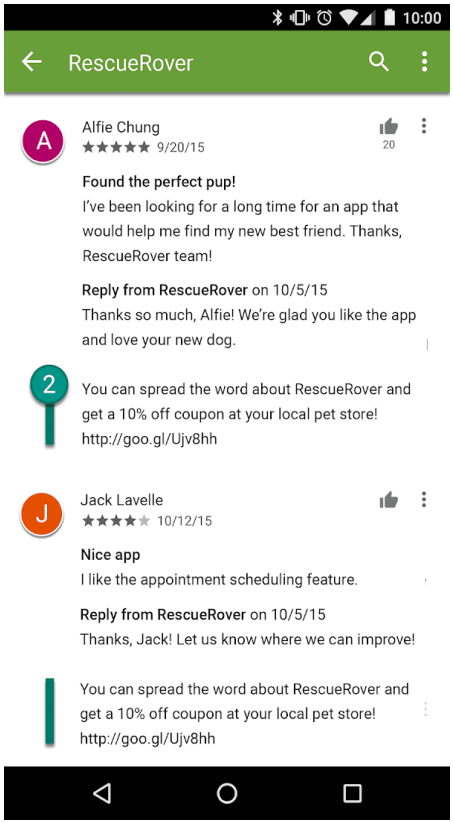
- Nutzer durch Incentives zur Bewertung Ihrer App bewegen:



① In dieser Benachrichtigung wird Nutzern ein Rabatt als Dankeschön für eine gute Bewertung angeboten.

- Wiederholte Abgabe von Bewertungen als angeblicher Nutzer, um die Platzierung einer App bei Google Play zu beeinflussen

- Abgabe von Rezensionen oder Aufforderung zur Abgabe von Rezensionen mit unangemessenen Inhalten wie Partnerinhalten, Gutscheinen, Spielcodes, E-Mail-Adressen oder Links zu Websites oder anderen Apps:



② Diese Rezension fordert Nutzer durch ein Gutscheinangebot auf, Werbung für die RescueRover App zu machen.

Mit Bewertungen und Rezensionen messen wir die Qualität von Apps. Nutzer müssen sich darauf verlassen können, dass sie echt und relevant sind. Hier einige Best Practices zur Beantwortung von Nutzerrezensionen:

- Gehen Sie nur auf die in den Bemerkungen des Nutzers genannten Punkte ein und bitten Sie nicht um eine bessere Bewertung.
- Verweisen Sie auf hilfreiche Ressourcen wie die Adresse des Kundenservice oder FAQ-Seiten.

Altersfreigaben

Altersfreigaben bei Google Play werden von der International Age Rating Coalition (IARC) bereitgestellt und sollen Entwicklern dabei helfen, Nutzern lokal relevante Altersfreigaben zu vermitteln. Regionale IARC-Behörden erstellen Richtlinien, anhand derer die Altersstufe der Inhalte einer App bestimmt wird. Apps ohne Altersfreigabe sind bei Google Play nicht zulässig.

Zweck der Altersfreigabe

Die Altersfreigabe soll Konsumenten, insbesondere Eltern, dabei helfen, potenziell anstößige Inhalte in einer App zu erkennen. Zusätzlich können damit Ihre Inhalte für bestimmte Regionen oder Nutzer gefiltert oder blockiert werden, wenn dies gesetzlich vorgeschrieben ist. Außerdem kann die Eignung Ihrer App für spezielle Entwicklerprogramme festgestellt werden.

Entscheidung über die Altersfreigabe

Damit Sie eine Altersfreigabe erhalten, müssen Sie in der Play Console einen Fragebogen zur Altersfreigabe ausfüllen, in dem Sie Fragen zu den Inhalten Ihrer App beantworten. Auf der Basis Ihrer Antworten erhalten Sie dann von mehreren Bewertungsstellen eine Altersfreigabe. Eine

Falschdarstellung des Inhalts kann die Entfernung oder Sperrung Ihrer App zur Folge haben. Deshalb ist es wichtig, den Fragebogen korrekt zu beantworten.

Füllen Sie den Fragebogen zur Altersfreigabe für jede neue über die Developer Console eingereichte App sowie für alle vorhandenen, bei Google Play aktiven Apps aus. Ansonsten erhält Ihre App die Kennzeichnung "Nicht bewertet". Apps ohne Altersfreigabe werden aus dem Play Store entfernt.

Wenn Sie Änderungen am Inhalt Ihrer App oder an Funktionen vornehmen, die Einfluss auf die Antworten im Fragebogen haben, müssen Sie einen neuen Fragebogen in der Play Console einreichen.

In der Hilfe finden Sie weitere Informationen zu den unterschiedlichen Bewertungsstellen und zum Ausfüllen des Fragebogens.

Beschwerde gegen eine Altersfreigabe

Wenn Sie mit der Altersfreigabe Ihrer App nicht einverstanden sind, können Sie direkt bei der entsprechenden IARC-Bewertungsstelle Einspruch erheben. Klicken Sie dazu auf den Link in der E-Mail mit dem Bewertungszertifikat.

Nachrichten

Eine Nachrichten-App ist eine App, die

- in der Google Play Console als Nachrichten-App deklariert ist oder
- im Google Play Store unter der Kategorie „Nachrichten & Zeitschriften“ aufgeführt ist und in Titel, Symbol, Entwicklernamen oder Beschreibung der App mit „Nachrichten“ beschrieben wird.

Beispiele für Apps aus der Kategorie „Nachrichten & Zeitschriften“, die als Nachrichten-Apps eingestuft werden:

- Apps, die in ihren Beschreibungen als „Nachrichten“ bezeichnet werden, darunter:
  - Aktuelle Nachrichten
  - Zeitungen
  - Eilmeldungen
  - Lokalnachrichten
  - Nachrichten des Tages
- Apps mit dem Wort „Nachrichten“ im Titel, Symbol oder Entwicklernamen

Apps, die hauptsächlich von Nutzern erstellte Inhalte enthalten (z. B. Apps für soziale Medien), dürfen nicht als Nachrichten-Apps deklariert werden und werden auch nicht entsprechend eingestuft.

Nachrichten-Apps, für die ein Nutzer eine Mitgliedschaft erwerben muss, müssen Nutzern vor dem Kauf eine In-App-Inhaltsvorschau bieten.

Nachrichten-Apps müssen

- Angaben zu Eigentumsrechten an der App und der Quelle der Nachrichtenartikel machen, einschließlich, aber nicht beschränkt auf den ursprünglichen Verlag, Webpublisher oder Autor des jeweiligen Artikel. Wo es nicht üblich ist, die einzelnen Autoren der Artikel aufzuführen, muss der ursprüngliche Verlag oder Webpublisher der Artikel die Nachrichten-App selbst sein. Beachten Sie, dass Links zu Konten in sozialen Medien nicht als Angabe zu Autor, Verlag oder Webpublisher ausreichen.
- eine spezielle Website oder In-App-Seite bieten, die deutlich als Kontaktdaten enthaltend gekennzeichnet ist, die leicht zu finden ist (z. B. über einen Link unten auf der Startseite oder in der Navigationsleiste der Website) und die gültige Kontaktdaten für den Nachrichtenverlag enthält, darunter entweder eine E-Mail-Adresse oder Telefonnummer. Beachten Sie, dass Links zu Konten in sozialen Medien keine ausreichende Form von Kontaktdaten darstellen.

Nachrichten-Apps dürfen

- keine erheblichen Rechtschreib- oder Grammatikfehler enthalten,
- nicht nur statischen Content enthalten, z. B. Inhalte, die mehrere Monate alt sind,
- Affiliate-Marketing oder Werbeeinnahmen nicht als primären Zweck haben.

Beachten Sie, dass Nachrichten-Apps Werbung und andere Formen von Marketing zur Monetarisierung verwenden *dürfen*, sofern der Hauptzweck der App nicht darin besteht, Produkte und Dienstleistungen zu verkaufen oder Werbeeinnahmen zu generieren.

Nachrichten-Apps, die Inhalte von verschiedenen Veröffentlichungsquellen zusammenfassen, müssen hinsichtlich der Veröffentlichungsquellen transparent sein und jede Quelle muss den Richtlinien für Nachrichten-Apps entsprechen.

In diesem Artikel erfahren Sie, wie Sie uns die erforderlichen Informationen am besten zukommen lassen können.

Spam und Mindestanforderungen an die Funktionalität

In jedem Fall sollten Apps den Nutzern ein grundlegendes Maß an Funktionalität und eine von Respekt geprägte Nutzererfahrung bieten. Apps, die abstürzen, ein Verhalten an den Tag legen, das dem Nutzer keinen funktionalen Mehrwert bietet, oder deren Zweck allein im Spamming von Nutzern oder Google Play besteht, stellen keine sinnvolle Ergänzung des Katalogs dar.

Spam

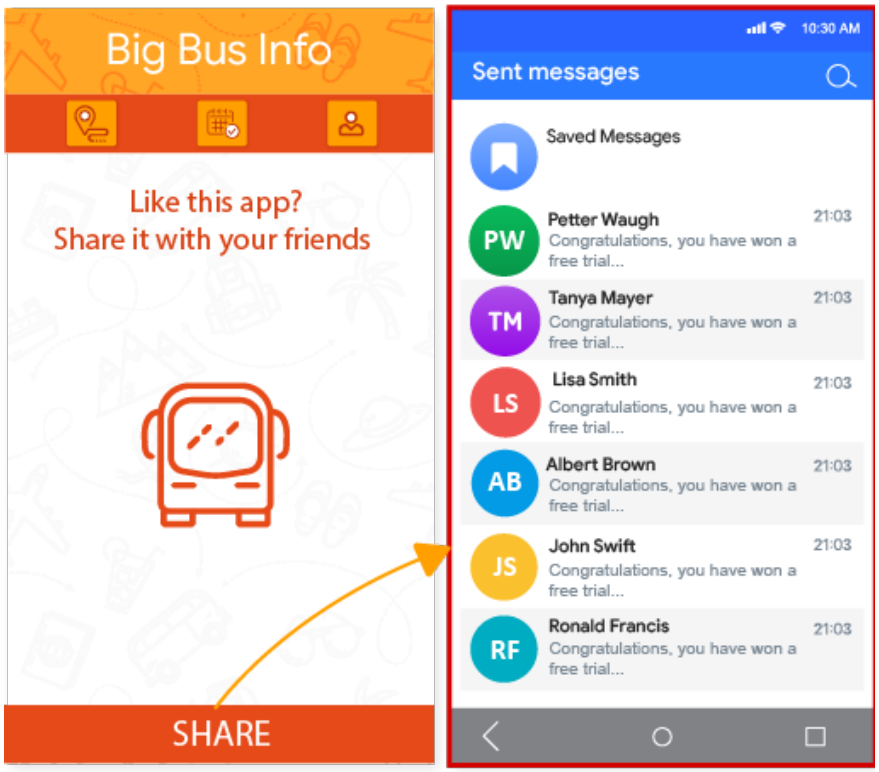
Wir gestatten keine Apps, die Nutzer oder Google Play spammen, etwa Apps, die Nutzern unerwünschte Nachrichten senden, sowie sich wiederholende und minderwertige Apps.

Spam in SMS, MMS und E-Mails

Apps, die SMS, E-Mails oder andere Nachrichten im Namen eines Nutzers senden, ohne diesem die Möglichkeit zu geben, Inhalt und Empfänger zu bestätigen, sind nicht zulässig.

Da Google Play eine sichere und respektvolle Plattform bleiben soll, haben wir Richtlinien entwickelt, in denen schädliche oder unangemessene Inhalte definiert und verboten werden.

- Wenn der Nutzer auf die Schaltfläche „Teilen“ tippt, sendet die App Nachrichten im Namen des Nutzers, ohne dass dieser die Möglichkeit hat, den Inhalt und die Empfänger zu bestätigen:

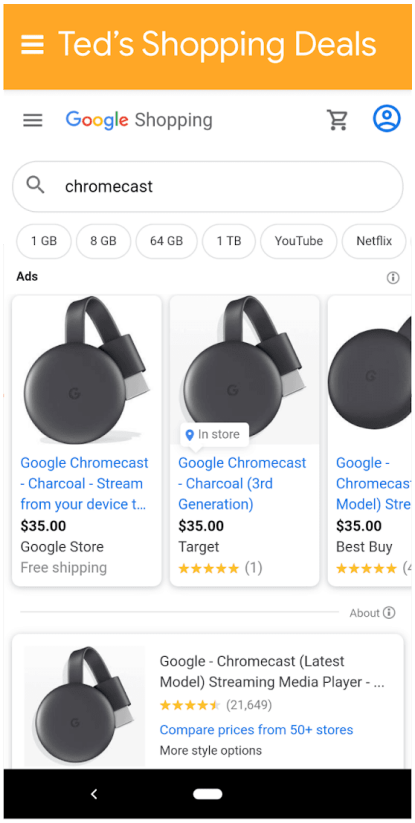


Spam zum Generieren von Seitenzugriffen und Affiliate-Spam

Apps, die in erster Linie Zugriffe auf Partnerwebsites generieren oder eine Webansicht einer Website bereitstellen, ohne die Zustimmung des jeweiligen Websiteinhabers oder -administrators eingeholt zu haben, sind nicht zulässig.

Da Google Play eine sichere und respektvolle Plattform bleiben soll, haben wir Richtlinien entwickelt, in denen schädliche oder unangemessene Inhalte definiert und verboten werden.

- Eine App, die in erster Linie Verweiszugriffe auf eine Website generieren soll, um Gutschriften für Anmeldungen oder Käufe von Nutzern auf dieser Website zu erhalten
- Apps, die in erster Linie eine Webansicht einer Website bereitstellen, ohne die erforderliche Zustimmung eingeholt zu haben:



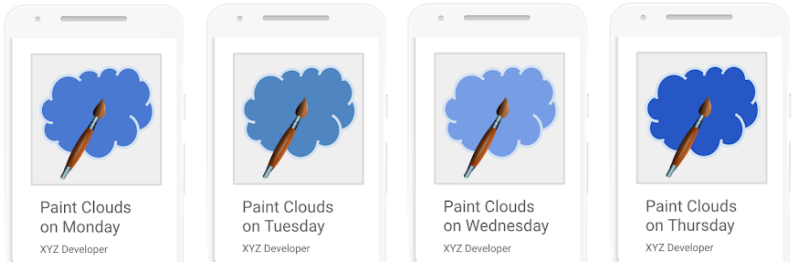
① Die App heißt „Ted's Shopping Deals", zeigt aber lediglich eine Webansicht von Google Shopping.

Sich wiederholende Inhalte

Wir gestatten keine Apps, deren Inhalte oder Funktionen denen von Apps entsprechen, die bereits bei Google Play angeboten werden. Apps müssen einzigartige Inhalte oder Funktionen enthalten, um Nutzern einen Mehrwert zu bieten.

Da Google Play eine sichere und respektvolle Plattform bleiben soll, haben wir Richtlinien entwickelt, in denen schädliche oder unangemessene Inhalte definiert und verboten werden.

- Das Kopieren aus anderen Apps, ohne eigene Inhalte hinzuzufügen oder einen Mehrwert zu bieten.
- Das Erstellen mehrerer Apps mit sehr ähnlichen Inhalten und Funktionen. Enthalten die einzelnen Apps jeweils wenig Inhalt, sollten Entwickler eventuell eine App erstellen, in der alle Inhalte zusammengeführt werden.

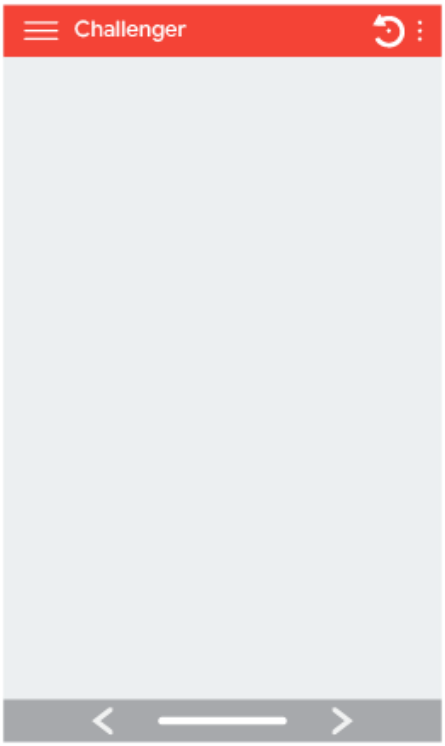


Mindestanforderungen an die Funktionalität

Ihre App sollte stabil sein, Interesse wecken und wie vom Nutzer erwartet reagieren.

Da Google Play eine sichere und respektvolle Plattform bleiben soll, haben wir Richtlinien entwickelt, in denen schädliche oder unangemessene Inhalte definiert und verboten werden.

- Apps, die keinen Zweck erfüllen oder keine Funktion haben



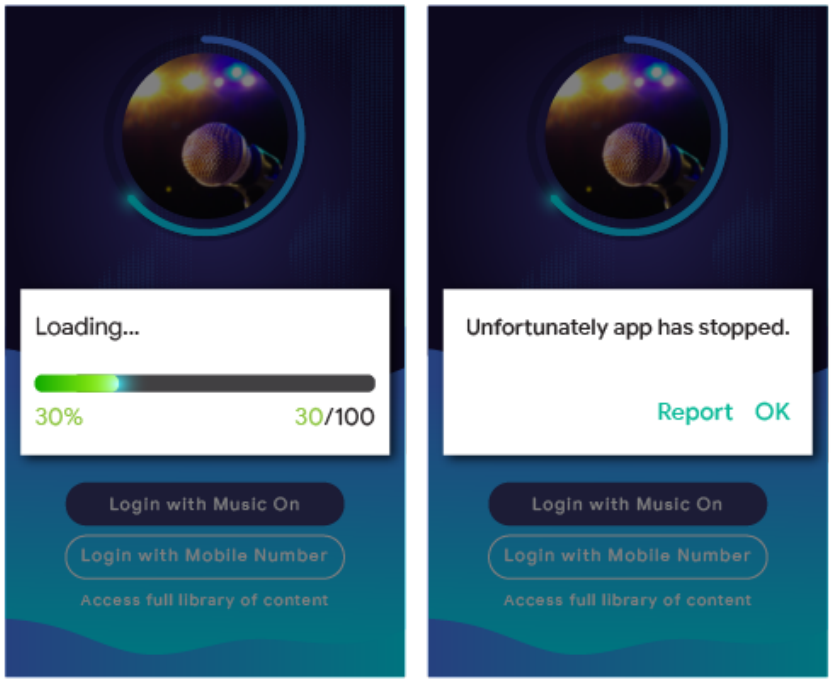
Fehlerhafte Funktionen

Apps, die abstürzen, ein Schließen erzwingen, sich aufhängen oder sonstige Auffälligkeiten zeigen, sind nicht zulässig.

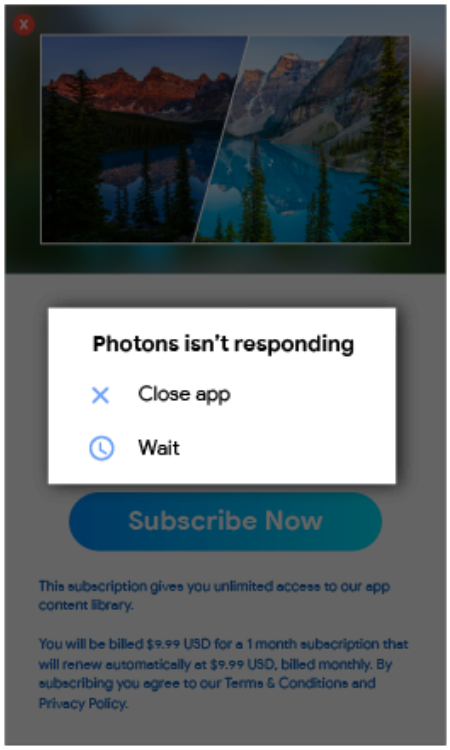
Da Google Play eine sichere und respektvolle Plattform bleiben soll, haben wir Richtlinien entwickelt, in denen schädliche oder unangemessene Inhalte definiert und verboten werden.

- Apps, die **nicht installiert werden können**

- Apps, die installiert, aber **nicht geladen werden können**



- Apps, die geladen werden können, aber **nicht reagieren**



Andere Programme

Apps, die für andere Android-Aktivitäten entwickelt wurden und über Google Play vertrieben werden, müssen nicht nur die Inhaltsrichtlinien erfüllen, die an anderer Stelle in dieser Richtlinienübersicht

aufgeführt sind, sondern unterliegen unter Umständen auch programmspezifischen Richtlinien. Prüfen Sie in der unten stehenden Liste, ob eine dieser Richtlinien für Ihre App gilt.

Android Instant Apps

Mit Android Instant Apps möchten wir für eine angenehme und nahtlose Nutzererfahrung sorgen und zugleich den höchsten Datenschutz- und Sicherheitsstandards gerecht werden. Unsere Richtlinien sind auf dieses Ziel ausgerichtet.

Entwickler, die Android Instant Apps bei Google Play vertreiben, müssen sich an die folgenden Richtlinien und alle anderen Google Play-Programmrichtlinien für Entwickler halten.

Identität

Bei Instant-Apps mit Anmeldefunktion muss Smart Lock für Passwörter implementiert werden.

Link-Unterstützung

Entwickler von Android Instant Apps müssen Links zu anderen Apps hinreichend unterstützen. Wenn Instant-Apps oder installierte Apps eines Entwicklers Links enthalten, die zu einer Instant-App weiterleiten können, muss der Entwickler die Nutzer zu dieser Instant-App weiterleiten, anstatt die Links beispielsweise in einem WebView aufzunehmen .

Technische Daten

Entwickler müssen die technischen Spezifikationen und Anforderungen von Android Instant Apps wie von Google angegeben erfüllen, einschließlich der von uns öffentlich dokumentierten . Alle Spezifikationen und Anforderungen können von Zeit zu Zeit geändert werden.

App-Installation anbieten

Über die Instant-App kann Nutzern die Installation der App ermöglicht werden, allerdings darf dies nicht der Hauptzweck der Instant-App sein. Entwickler, die eine App-Installation anbieten, müssen Folgendes beachten:

- Das Material Design-Symbol "App herunterladen" und das Label "Installieren" dürfen nicht für die Installationsschaltfläche verwendet werden.
- In der Instant-App dürfen nicht mehr als zwei oder drei Installationsaufforderungen angezeigt werden.
- Entwickler dürfen kein Banner und keine andere anzeigenähnliche Methode verwenden, um Nutzer zur Installation aufzufordern.

Weitere Informationen zu Instant-Apps und UX-Richtlinien finden Sie in den Best Practices für die Nutzererfahrung .

Gerätestatus ändern

Instant-Apps dürfen am Gerät des Nutzers keine Änderungen vornehmen, die länger als die App-Sitzung andauern. Beispielsweise dürfen Apps nicht den Hintergrund des Nutzers ändern oder ein Startbildschirm-Widget erstellen.

Sichtbarkeit der App

Entwickler müssen darauf achten, dass Instant-Apps für den Nutzer sichtbar sind, sodass der Nutzer sich jederzeit bewusst ist, dass die App gerade auf dem Gerät ausgeführt wird.

Geräte-IDs

Instant-Apps dürfen keinen Zugriff auf Geräte-IDs erhalten, die 1) nach dem Ende der App-Sitzung weiterhin bestehen und 2) nicht vom Nutzer zurückgesetzt werden können. Beispiele:

- Build Serial
- MAC-Adressen auf Netzwerkchips
- IMEI, IMSI

Instant-Apps dürfen auf die Telefonnummer zugreifen, sofern diese während der Laufzeitberechtigung abgerufen wird. Entwickler dürfen nicht versuchen, den Nutzer anhand dieser IDs oder auf andere Weise zu identifizieren.

Netzwerkverkehr

Netzwerkverkehr aus der Instant-App muss mit einem TLS-Protokoll, beispielsweise HTTPS, verschlüsselt werden.

Richtlinie zu Emojis unter Android

Mit unserer Emoji-Richtlinie wollen wir ein Zeichen für Inklusion setzen und eine einheitliche Darstellung für alle Nutzer ermöglichen. Dazu müssen sämtliche Apps die aktuelle Version von Unicode Emoji unterstützen, wenn sie unter Android 12 und höher laufen.

Apps, die die Standard-Android-Emojis ohne eigene Implementierungen verwenden, nutzen bereits die aktuelle Version von Unicode Emoji, wenn sie unter Android 12 und höher laufen.

Apps mit eigenen Emoji-Implementierungen, einschließlich von Bibliotheken von Drittanbietern, müssen aktuelle Unicode Emoji-Versionen innerhalb von vier Monaten nach deren Veröffentlichung in vollem Umfang unterstützen, wenn sie unter Android 12 und höher laufen.

In dieser Anleitung finden Sie Informationen zur Unterstützung moderner Emoji.

Verwenden Sie die folgenden Emoji-Beispiele, um zu testen, ob Ihre App mit der aktuellen Unicode-Version kompatibel ist:

Beispiele	Unicode-Version
🩷 🤳 🐓	15.0
🫠 🫱🏻 🫵🏾	14.0
😶‍🌫️ 👩🏻 👩🏻‍❤️‍👩🏻	13.1
🥲 🫜 🐻‍❄️	13.0
🧑‍🦰 🚶 👫	12.1
🦩 🫀 👭	12.0

Familienfreundliche Inhalte

Google Play bietet Entwicklern eine funktionsreiche Plattform zur Präsentation erstklassiger, altersgemäßer Inhalte für die ganze Familie. Vor der Einreichung einer App an das Designed for Families-Programm bzw. der Einreichung einer App für Kinder an den Google Play Store müssen Sie dafür sorgen, dass die App für Kinder geeignet ist und alle relevanten Gesetze eingehalten werden.

Hier können Sie mehr über den Einreichungsprozess für Designed for Families erfahren und die interaktive Checkliste der Academy for App Success durchgehen.

Google Play-Richtlinien für familienfreundliche Inhalte

Technologie wird immer häufiger dazu verwendet, das Familienleben zu bereichern. Eltern interessieren sich daher für sichere, qualitativ ansprechende Inhalte, die sie mit ihren Kindern teilen können. Womöglich entwickeln Sie Apps speziell für Kinder oder aber Sie erregen damit deren

Aufmerksamkeit. Google Play möchte Ihnen dabei helfen, Ihre App für alle Nutzer, einschließlich Familien, sicher zu gestalten.

Das Wort „Kinder“ kann in unterschiedlichen Sprachen und unterschiedlichen Zusammenhängen verschiedene Bedeutungen haben. Es ist wichtig, dass Sie sich von Ihrem Rechtsbeistand dahingehend beraten lassen, welche Verpflichtungen und/oder altersbedingten Einschränkungen für Ihre App gelten. Sie selbst wissen am besten, wie Ihre App funktioniert. Deshalb benötigen wir Ihre Unterstützung, um dafür sorgen zu können, dass Apps bei Google Play für Familien sicher sind.

Für alle Apps, die die Google-Richtlinien für familienfreundliche Inhalte einhalten, kann eine Einstufung als von Pädagogen empfohlene App beantragt werden. Wir können jedoch nicht gewährleisten, dass Ihre App auch entsprechend eingestuft wird.

Vorgaben zur Nutzung der Play Console

Zielgruppe und Inhalte

Im Bereich Zielgruppe und Inhalte der Google Play Console müssen Sie vor der Veröffentlichung Ihrer App deren Zielgruppe angeben, indem Sie eine Altersgruppe aus der Liste auswählen. Wenn Sie in Ihrer App Bilder oder Begriffe verwenden, die potenziell auf Kinder ausgerichtet sind, hat dies unter Umständen Auswirkungen auf die Prüfung der von Ihnen angegebenen Zielgruppe durch Google Play – unabhängig davon, welche Angaben Sie in der Google Play Console gemacht haben. Google Play behält sich das Recht vor, die von Ihnen zur Verfügung gestellten App-Informationen selbst zu überprüfen, um feststellen zu können, ob Ihre Angaben hinsichtlich der Zielgruppe korrekt sind.

Wenn Sie eine Zielgruppe auswählen, die nur Erwachsene umfasst, und Google feststellt, dass dies nicht den Tatsachen entspricht, da Ihre App sowohl auf Kinder als auch auf Erwachsene ausgerichtet ist, können Sie zustimmen, dass die App ein Label erhält, mit dem Nutzer gewarnt werden, dass die App nicht für Kinder bestimmt ist.

Sie sollten nur dann mehr als eine Altersgruppe als Zielgruppe auswählen, wenn die App für Nutzer dieser Altersgruppen entwickelt wurde und auch wirklich für sie geeignet ist. Beispiel: Bei Apps, die für Babys, Kleinkinder und Kinder im Vorschulalter entwickelt wurden, sollte nur die Altersgruppe "5 Jahre und jünger" ausgewählt werden. Wenn Ihre App für Kinder bestimmter Klassenstufen entwickelt wurde, wählen Sie die Altersgruppe aus, die der Stufe am ehesten entspricht. Wählen Sie nur dann Altersgruppen aus, die sowohl Erwachsene als auch Kinder umfassen, wenn Ihre App auch tatsächlich für alle Altersstufen entwickelt wurde.

Aktualisierung des Bereichs "Zielgruppe und Inhalte"

Sie können die App-Informationen im Bereich "Zielgruppe und Inhalte" jederzeit in der Google Play Console aktualisieren. Damit diese Informationen im Google Play Store angezeigt werden, ist ein App-Update erforderlich. Unter Umständen wird jedoch bei allen Änderungen in diesem Bereich der Google Play Console noch vor einem App-Update geprüft, ob sie den jeweiligen Richtlinien entsprechen.

Wir empfehlen dringend, Ihre bestehenden Nutzer darüber zu informieren, wenn Sie die Zielgruppe Ihrer App ändern oder damit anfangen, Werbeanzeigen bzw. In-App-Käufe zu verwenden. Nutzen Sie dazu entweder den Bereich "Neuigkeiten" auf der Store-Eintragsseite der App oder In-App-Benachrichtigungen.

Falschdarstellung in der Play Console

Werden Informationen in der Play Console falsch dargestellt, einschließlich des Bereichs "Zielgruppe und Inhalte", kann das zur Entfernung oder Sperrung Ihrer App führen. Deshalb ist es wichtig, korrekte Angaben zu machen.

Anforderungen der Richtlinie für familienfreundliche Inhalte

Wenn eine der Zielgruppen Ihrer App Kinder sind, müssen Sie die folgenden Anforderungen erfüllen. Andernfalls kann Ihre App entfernt oder gesperrt werden.

1. **App-Inhalte**: App-Inhalte, die für Kinder zugänglich sind, müssen für sie geeignet sein. Wenn Ihre App Inhalte enthält, die zwar nicht weltweit, aber in einer bestimmten Region als für minderjährige Nutzer geeignet eingestuft werden, ist die App unter Umständen in dieser Region verfügbar (eingeschränkte Regionen). In allen anderen Regionen ist sie nicht verfügbar.
2. **App-Funktionalität**: Ihre App darf nicht nur eine Webansicht einer Website darstellen oder dem Hauptzweck dienen, Nutzer ohne Berechtigung durch den Websiteinhaber oder Administrator auf Affiliate-Websites weiterzuleiten.
3. **Antworten in der Play Console**: Sie müssen die in der Play Console gestellten Fragen zu Ihrer App korrekt beantworten und diese Antworten bei Änderungen der App entsprechend aktualisieren. Unter anderem müssen Sie korrekte Angaben zu Ihrer App im Abschnitt zur Zielgruppe, zum Inhalt und zur Datensicherheit und im Fragebogen zur IARC-Altersfreigabe machen.
4. **Datennutzung**: Sie müssen die Erhebung jeglicher personenbezogener und vertraulicher Daten von Kindern durch Ihre App offenlegen. Das gilt auch für APIs und SDKs, die in der App aufgerufen oder genutzt werden. Zu diesen vertraulichen Daten gehören unter anderem Authentifizierungsinformationen, Daten von Mikrofon- und Kamerasensoren, Geräte- und Werbenutzungsdaten sowie die Android-ID. Außerdem müssen Sie mit Ihrer App die folgenden Regeln zur Datennutzung einhalten:
   - Apps, die ausschließlich für Kinder bestimmt sind, dürfen keine Android-Werbe-ID (Android Advertising Identifier, AAID), SIM-Seriennummer, Build-Seriennummer, BSSID, MAC-Adresse, SSID, IMEI und/oder IMSI übertragen.
     - Apps, die ausschließlich für Kinder bestimmt sind, sollten nicht die Berechtigung „Werbe-ID“ beantragen, wenn sie für Android API 33 oder höher ausgelegt sind.
   - Apps, die sowohl auf Kinder als auch ältere Zielgruppen ausgerichtet sind, dürfen keine AAID, SIM-Seriennummer, Build-Seriennummer, BSSID, MAC-Adresse, SSID, IMEI und/oder IMSI von Kindern oder Nutzern unbekannten Alters übertragen.
   - Telefonnummern des Geräts dürfen nicht über TelephonyManager der Android API angefordert werden.
   - Apps, die ausschließlich für Kinder bestimmt sind, dürfen weder die Berechtigung zur Standortermittlung anfordern noch den genauen Standort des Nutzers erheben, verwenden oder übertragen.
   - Apps müssen den Companion Device Manager (CDM) verwenden, wenn sie die Berechtigung für Bluetooth anfragen, außer sie wurden ausschließlich für Betriebssystemversionen entwickelt, die mit dem CDM nicht kompatibel sind.
5. **APIs und SDKs**: APIs und SDKs müssen ordnungsgemäß in Ihrer App implementiert sein.
   - Apps, die ausschließlich für Kinder bestimmt sind, dürfen keine APIs oder SDKs enthalten, die nicht für die Verwendung in primär auf Kinder ausgerichteten Diensten zugelassen sind.
     - Ein API-Dienst, bei dem OAuth-Technologie zur Authentifizierung und Autorisierung eingesetzt wird und der laut seinen Nutzungsbedingungen nicht für die Verwendung in auf Kinder ausgerichteten Diensten zugelassen ist, ist ein Beispiel hierfür.
   - In Apps, die sowohl für Kinder als auch für ältere Nutzer bestimmt sind, dürfen keine APIs oder SDKs implementiert werden, die nicht für die Verwendung in auf Kinder ausgerichteten Diensten zugelassen sind – es sei denn, sie werden hinter einer neutralen Altersabfrage eingesetzt oder so implementiert, dass durch sie keine Daten von Kindern erhoben werden. Bei Apps, die sowohl auf Kinder als auch auf ältere Zielgruppen ausgerichtet sind, dürfen zum Zugriff auf App-Inhalte durch Nutzer keine APIs oder SDKs zum Einsatz kommen, die nicht für die Verwendung in auf Kinder ausgerichteten Diensten zugelassen sind.
6. **Augmented Reality (AR)**: Wenn Sie in Ihrer App Augmented Reality verwenden, ist beim Start des AR-Bereichs sofort eine Sicherheitswarnung einzublenden. Dieser Warnhinweis sollte Folgendes enthalten:

- Eine entsprechende Benachrichtigung, in der die Wichtigkeit der Elternaufsicht betont wird
- Eine Erinnerung daran, sich physischer Gefahren in der realen Welt bewusst zu sein, beispielsweise der eigenen Umgebung
- Die Nutzung Ihrer App muss ohne ein Gerät möglich sein, das nicht für Kinder empfohlen ist (z. B. Daydream oder Oculus).

7. **Social Apps und Funktionen für soziale Netzwerke**: Wenn Nutzer die Möglichkeit haben, in Ihren Apps Informationen zu teilen oder auszutauschen, müssen Sie die entsprechenden Funktionen im Fragebogen zur Altersfreigabe in der Play Console genau angeben.
   - Social Apps: Dies sind Apps, deren Hauptfunktion darin besteht, Nutzern zu ermöglichen, selbst gewählte Inhalte mit großen Personengruppen zu teilen oder mit diesen zu kommunizieren. In allen Social Apps, die auch für Kinder gedacht sind, muss ein Hinweis zum sicheren Verhalten im Internet und zu den realen Gefahren der Internetnutzung angezeigt werden, bevor Kindern der Austausch von selbst gewählten Medien oder Informationen gestattet wird. Darüber hinaus müssen Sie die Bestätigung durch einen Erwachsenen verlangen, bevor Sie Kindern den Austausch von personenbezogenen Daten gestatten.
   - Funktionen für soziale Netzwerke: Eine Funktion für soziale Netzwerke ist eine zusätzliche App-Funktion, die es Nutzern ermöglicht, selbst gewählte Inhalte mit großen Personengruppen zu teilen oder mit diesen zu kommunizieren. In einer App, die auch für Kinder gedacht ist und Funktionen für soziale Netzwerke besitzt, muss ein Hinweis zum sicheren Verhalten im Internet und zu den realen Gefahren der Internetnutzung angezeigt werden, bevor Kindern der Austausch eigener und freier Inhalte oder Informationen gestattet wird. Zusätzlich müssen Sie eine Methode anbieten, mit der Erwachsene die Funktionen für soziale Netzwerke für Kinder verwalten können. Hierzu zählen auch die Aktivierung bzw. Deaktivierung der Funktionen für soziale Netzwerke und die Festlegung des Funktionsumfangs. Außerdem müssen Sie die Bestätigung durch einen Erwachsenen verlangen, bevor Funktionen aktiviert werden, mit denen Kinder personenbezogene Daten austauschen können.
   - „Bestätigung durch einen Erwachsenen“ bezeichnet eine Methode, mit der bestätigt werden kann, dass der Nutzer kein Kind ist, und mit der Kinder nicht dazu ermutigt werden, ein falsches Alter anzugeben, um Zugang zu App-Bereichen zu erlangen, die für Erwachsene bestimmt sind. Bestätigungsmethoden können eine PIN, ein Passwort, ein Geburtsdatum, eine E-Mail-Bestätigung, ein Lichtbildausweis, eine Kreditkarte oder eine Sozialversicherungsnummer eines Erwachsenen sein.
   - Social Apps, die vorwiegend dazu dienen, mit unbekannten Personen zu chatten, dürfen Kinder nicht als Zielgruppe haben. Beispiele hierfür sind Apps im Stil von Chat Roulette, Dating-Apps und offene Chatrooms, die sich vorwiegend an Kinder richten.

8. **Einhaltung gesetzlicher Bestimmungen**: Sie müssen dafür sorgen, dass Ihre App – einschließlich aller APIs und SDKs, die darin aufgerufen oder eingesetzt werden – nicht gegen das US-Gesetz zum Schutz der Privatsphäre von Kindern im Internet (Children's Online Privacy Protection Act, COPPA) , die EU-Datenschutz-Grundverordnung (DSGVO) oder sonstige geltende Gesetze oder Bestimmungen verstößt.

Da Google Play eine sichere und respektvolle Plattform bleiben soll, haben wir Richtlinien entwickelt, in denen schädliche oder unangemessene Inhalte definiert und verboten werden.

- Apps, in deren Store-Eintrag Spiele für Kinder beworben werden, deren Inhalte jedoch nur für Erwachsene geeignet sind
- Apps, in denen APIs implementiert sind, deren Nutzungsbedingungen den Einsatz in auf Kinder ausgerichteten Apps verbieten
- Apps, in denen der Konsum von Alkohol, Tabak oder Betäubungsmitteln verherrlicht wird
- Apps, die echte oder simulierte Glücksspiele beinhalten
- Apps mit Gewaltdarstellungen, Blut oder schockierenden Inhalten, die für Kinder nicht geeignet sind
- Dating-Apps oder Apps, in denen Ratschläge zu den Themen Sexualität und Partnerschaft erteilt werden

- Apps, die Links zu Websites enthalten, deren Inhalte gegen die Google Play-Programmrichtlinien für Entwickler verstoßen
- Apps, in denen Kindern nicht jugendfreie Werbung präsentiert wird, beispielsweise gewaltverherrlichende Inhalte, sexuelle Inhalte oder glücksspielbezogene Inhalte

Anzeigen und Monetarisierung

Wenn Sie eine App, die auf Kinder ausgerichtet ist, bei Google Play monetarisieren, muss sie die folgenden Anforderungen der Richtlinien zu Anzeigen und Monetarisierung in familienfreundlichen Apps erfüllen.

Die Richtlinien weiter unten gelten für alle Monetarisierungs- und Werbemaßnahmen in Ihrer App, einschließlich Werbeanzeigen, Cross-Promotions sowohl für Ihre eigenen Apps als auch für Drittanbieter-Apps, In-App-Kaufangeboten sowie allen sonstigen kommerziellen Inhalten, wie z. B. bezahlten Produktplatzierungen. Jegliche Monetarisierungs- und Werbemaßnahmen in diesen Apps müssen allen geltenden Gesetzen und Vorschriften entsprechen, einschließlich aller relevanten Richtlinien zur freiwilligen Selbstkontrolle und Branchenrichtlinien.

Google Play behält sich das Recht vor, Apps aufgrund übermäßig aggressiver Werbepraktiken abzulehnen, zu entfernen oder zu sperren.

Anforderungen an Anzeigen

Wenn Kindern oder Nutzern unbekannten Alters in Ihrer App Werbeanzeigen präsentiert werden, ist Folgendes zu beachten:

- Verwenden Sie nur selbstzertifizierte Anzeigen-SDKs von Google Play für familienfreundliche Inhalte, um diesen Nutzern Werbung zu präsentieren
- Werbung, die diesen Nutzern angezeigt wird, darf weder interessenbezogen sein (Werbung, die basierend auf ihrem Online-Browserverhalten auf einzelne Nutzer mit bestimmten Eigenschaften ausgerichtet ist) noch Remarketing (Werbung, die basierend auf vorherigen Interaktionen mit einer App oder Website auf einzelne Nutzer ausgerichtet ist) beinhalten
- Werbeinhalte, die diesen Nutzern angezeigt werden, müssen für Kinder geeignet sein
- Werbung, die diesen Nutzern angezeigt wird, muss den Formatanforderungen für Werbeanzeigen in familienfreundlichen Apps entsprechen
- Alle geltenden rechtlichen Vorschriften und Branchenstandards im Hinblick auf Werbeinhalte für Kinder müssen erfüllt werden

Anforderungen an Anzeigenformate

Die Monetarisierung und die Werbung in Ihrer App dürfen keine irreführenden Inhalte aufweisen und auch nicht so konzipiert sein, dass minderjährige Nutzer versehentlich darauf klicken könnten.

Wenn die Zielgruppe Ihrer App ausschließlich Kinder sind, ist Folgendes verboten. Wenn die Zielgruppe Ihrer App sowohl Kinder als auch ältere Personen sind, ist Folgendes verboten, wenn Werbeanzeigen für Kinder oder Nutzer unbekannten Alters ausgeliefert werden:

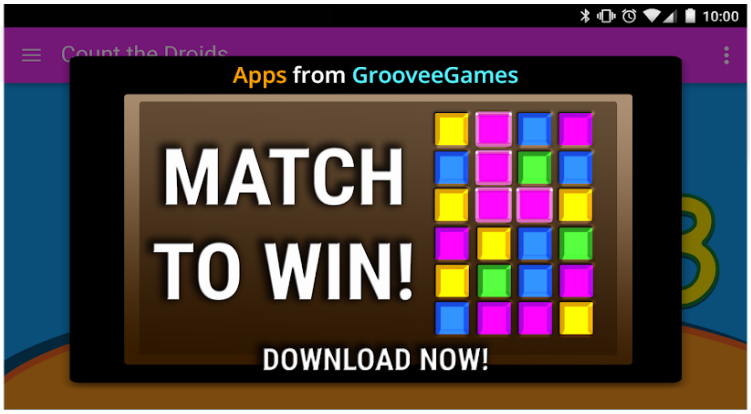
- Störende Monetarisierung und Werbung einschließlich solcher, die den gesamten Bildschirm einnehmen oder die normale Nutzung beeinträchtigen und keine klar ersichtliche Möglichkeit bieten, die Werbeanzeigen auszublenden (z. B. blockierende Anzeigen).
- Monetarisierung und Werbung, die die normale Nutzung der App oder des Spiels beeinträchtigen, einschließlich Anzeigen mit Prämie oder Opt-in-Anzeigen, die nicht nach 5 Sekunden geschlossen werden können.
- Monetarisierung und Werbung, die die normale App-Nutzung oder das normale Spiel nicht beeinträchtigen, dürfen länger als 5 Sekunden eingeblendet werden, z. B. Videoinhalte mit integrierten Anzeigen.
- Interstitial-Anzeigen zur Monetarisierung und Werbung, die direkt beim Start der App eingeblendet werden.

- Mehrere Anzeigen-Placements auf einer Seite (z. B. Banneranzeigen, die mehrere Angebote in einem Placement enthalten, oder mehrere Banner- oder Videoanzeigen) sind nicht zulässig.
- Monetarisierung und Werbung, die sich nicht klar von Ihren App-Inhalten unterscheiden lassen.
- Verwendung von schockierenden Inhalten oder emotional manipulativen Praktiken, die Nutzer dazu verleiten sollen, Anzeigen aufzurufen oder In-App-Käufe vorzunehmen.
- Eine fehlende Unterscheidung zwischen der Verwendung von virtuellen Spielmünzen und echtem Geld für In-App-Käufe.

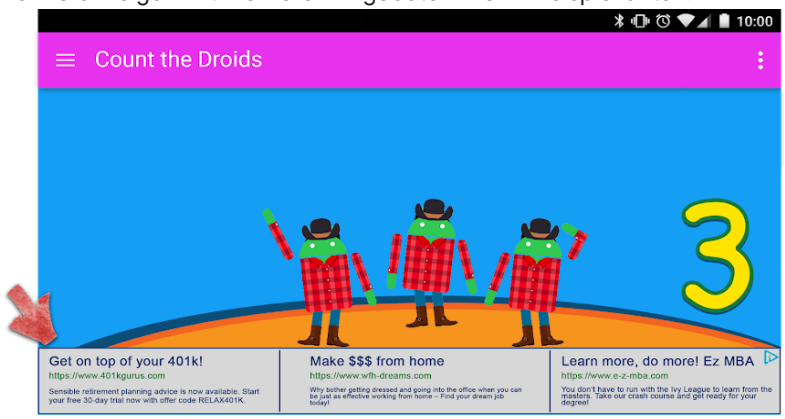
Da Google Play eine sichere und respektvolle Plattform bleiben soll, haben wir Richtlinien entwickelt, in denen schädliche oder unangemessene Inhalte definiert und verboten werden.

- Monetarisierung und Werbung, die sich vom Finger des Nutzers wegbewegen, wenn dieser versucht, sie zu schließen
- Monetarisierung und Werbung, die wie im Beispiel unten dem Nutzer keine Möglichkeit bieten, das Angebot nach fünf (5) Sekunden zu schließen:

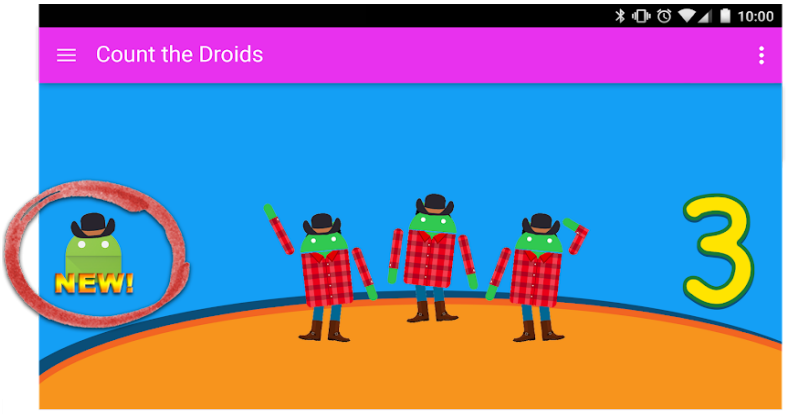
- Monetarisierung und Werbung, die sich wie im Beispiel unten über einen Großteil des Bildschirms erstrecken und bei denen die Schaltfläche zum Schließen nicht deutlich sichtbar ist:



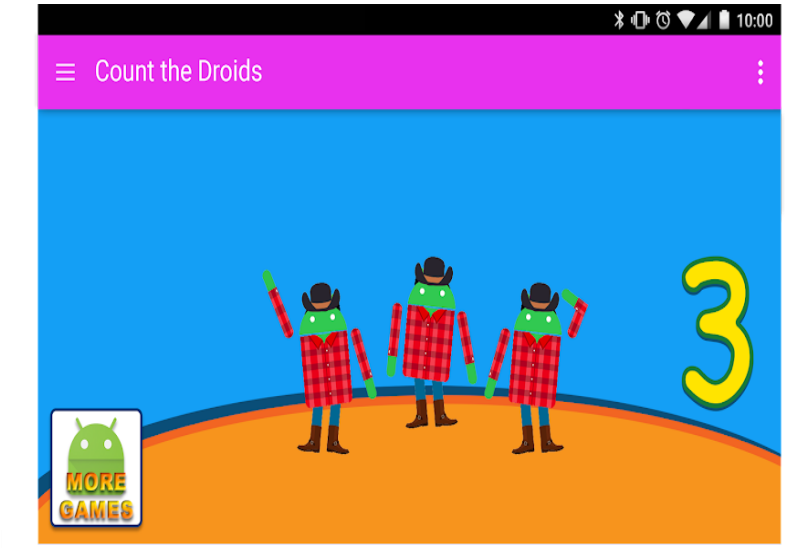
- Banneranzeigen mit mehreren Angeboten wie im Beispiel unten:



- Monetarisierung und Werbung wie im Beispiel unten, die der Nutzer fälschlicherweise für App-Inhalte halten könnte:



- Schaltflächen, Werbeanzeigen oder andere Formen der Monetarisierung wie im Beispiel unten, mit denen Ihre anderen Google Play Store-Einträge beworben werden, die sich jedoch nicht von App-Inhalten unterscheiden lassen:



Hier sind einige Beispiele für Anzeigeninhalte, die Kindern nicht eingeblendet werden dürfen.

- **Unangemessene Medieninhalte**: Werbung für Fernsehserien, Filme, Musikalben oder sonstige Medien, die für Kinder nicht geeignet sind.
- **Unangemessene Videospiele und herunterladbare Software**: Werbung für herunterladbare Software und elektronische Videospiele, die für Kinder nicht geeignet sind.

- **Betäubungsmittel oder schädliche Substanzen**: Werbung für Alkohol, Tabak, Betäubungsmittel und andere schädliche Substanzen.
- **Glücksspiel**: Werbung für simulierte Glücksspiele, Wettbewerbe oder Gewinnspiele – auch, wenn die Teilnahme kostenlos ist.
- **Nicht jugendfreie und sexuell anzügliche Inhalte**: Werbung mit pornografischen, sexuell anzüglichen und nicht jugendfreien Inhalten.
- **Dating oder Partnervermittlung**: Werbung für Dating- oder Partnervermittlungs-Websites.
- **Gewaltdarstellung**: Werbung mit Gewaltdarstellungen oder grausamen Inhalten, die für Kinder nicht geeignet sind.

Anzeigen-SDKs

Wenn Sie in Ihrer App Werbeanzeigen ausliefern und die App nur für Kinder bestimmt ist, dürfen Sie nur selbstzertifizierte Anzeigen-SDK-Versionen für familienfreundliche Inhalte verwenden. Ist die App sowohl für Kinder als auch für ältere Nutzer gedacht, müssen Sie Maßnahmen zur Feststellung des Alters ergreifen, beispielsweise eine neutrale Altersabfrage, und gewährleisten, dass Werbung, die Kindern präsentiert wird, ausschließlich von selbstzertifizierten Anzeigen-SDK-Versionen von Google Play stammt.

Weitere Informationen zu diesen Anforderungen erhalten Sie auf der Richtlinienseite zu selbstzertifizierten Anzeigen-SDKs für familienfreundliche Inhalte. Hier finden Sie eine aktuelle Liste der selbstzertifizierten Anzeigen-SDK-Versionen für familienfreundliche Inhalte.

Wenn Sie AdMob verwenden, besuchen Sie die AdMob-Hilfe, um weitere Details zu den entsprechenden Produkten zu erhalten.

Sie sind selbst dafür verantwortlich, dass Ihre App alle Anforderungen hinsichtlich Werbeanzeigen, In-App-Käufen und kommerziellen Inhalten erfüllt. Kontaktieren Sie die Anbieter Ihrer Anzeigen-SDKs, wenn Sie mehr über ihre Inhaltsrichtlinien und Werbepraktiken erfahren möchten.

Richtlinie für selbstzertifizierte Anzeigen-SDKs für familienfreundliche Inhalte

Google Play ist bestrebt, Kindern und Familien eine sichere Umgebung zur Verfügung zu stellen. Eine wesentliche Maßnahme in diesem Zusammenhang besteht darin, Kindern nur solche Werbeanzeigen zu präsentieren, die für ihr Alter geeignet sind, und dafür zu sorgen, dass ihre Daten ordnungsgemäß verarbeitet werden. Zu diesem Zweck verlangen wir von Anzeigen-SDKs und Vermittlungsplattformen eine Selbstzertifizierung, in der bestätigt wird, dass sie für Kinder geeignet sind und den Google Play-Programmrichtlinien für Entwickler und der Richtlinie für familienfreundliche Inhalte von Google Play entspricht, darunter auch den Anforderungen des Programms für selbstzertifizierte Anzeigen-SDKs für familienfreundliche Inhalte.

Das Programm für selbstzertifizierte Anzeigen-SDKs für familienfreundliche Inhalte von Google Play bietet Entwicklern eine wichtige Möglichkeit, festzustellen, welche Anzeigen-SDKs oder Vermittlungsplattformen selbst zertifiziert haben, dass sie für die Verwendung in speziell für Kinder entwickelten Apps geeignet sind.

Die Falschdarstellung von Informationen zu Ihrem SDK, einschließlich der Angaben in Ihrem Antragsformular, kann zur Entfernung oder Sperrung Ihres SDK aus dem Programm für selbstzertifizierte Anzeigen-SDKs für familienfreundliche Inhalte führen. Deshalb ist es wichtig, korrekte Angaben zu machen.

Richtlinienanforderungen

Wenn Ihr SDK oder Ihre Vermittlungsplattform Apps bereitstellt, die Teil des Google Play-Programms für familienfreundliche Inhalte sind, müssen die Google Play-Richtlinien für Entwickler sowie die folgenden Anforderungen eingehalten werden. Falls Richtlinienanforderungen nicht befolgt werden, kann dies zur Sperrung oder Entfernung aus dem Programm für selbstzertifizierte Anzeigen-SDKs für familienfreundliche Inhalte führen.

Sie sind dafür verantwortlich, dass bei Ihrem SDK oder Ihrer Vermittlungsplattform die Richtlinien befolgt werden. Bitte lesen Sie deshalb die Google Play-Programmrichtlinien für Entwickler , die Google Play-Richtlinien für familienfreundliche Inhalte sowie die Anforderungen des Programms für selbstzertifizierte Anzeigen-SDKs für familienfreundliche Inhalte .

1. **Anzeigeninhalte**: Anzeigeninhalte, die für Kinder zugänglich sind, müssen für sie geeignet sein.
   - Um dieses Ziel zu erfüllen, müssen Sie (i) Definitionen für anstößige Anzeigeninhalte und unangemessenes Verhalten festlegen und (ii) beides in Ihren Nutzungsbedingungen oder Richtlinien verbieten. Bei diesen Definitionen müssen die Google Play-Programmrichtlinien für Entwickler befolgt werden.
   - Sie müssen außerdem eine Methode entwickeln, mit der Sie Ihre Anzeigen danach einstufen können, ob sie sich für bestimmte Altersgruppen eignen. Dazu sollten in jedem Fall die Kategorien „Everyone“ (Jedes Alter) und „Mature“ (Nicht jugendfrei) gehören. Wenn für ein Anzeigen-SDK das Antragsformular ausgefüllt wurde, muss sich dessen Altersfreigabe-Methodik nach derjenigen richten, die Google für SDKs vorschreibt.
   - Wenn Sie Echtzeitgebote verwenden, um Werbeanzeigen an Kinder auszuliefern, müssen die Creatives überprüft worden sein und den oben genannten Anforderungen nachkommen.
   - Darüber hinaus müssen Creatives visuell kenntlich gemacht werden, die aus Ihrem Inventar stammen (z. B. durch ein Wasserzeichen Ihres Firmenlogos).
2. **Anzeigenformat**: Alle Anzeigen, die minderjährigen Nutzern präsentiert werden, müssen den Anforderungen an Anzeigenformate für Werbeanzeigen in familienfreundlichen Apps entsprechen. Außerdem müssen Sie Entwicklern das Auswählen von Anzeigenformaten ermöglichen, die die Google Play-Richtlinien für familienfreundliche Inhalte befolgen.
   - Werbeanzeigen dürfen keine irreführenden Inhalte haben. Außerdem dürfen sie nicht so gestaltet sein, dass Kinder zu unbeabsichtigten Klicks verleitet werden.
   - Störende Werbung einschließlich solcher, die den gesamten Bildschirm einnimmt oder von einer normalen Nutzung abhält und keine klar ersichtliche Möglichkeit bietet, die Werbung auszublenden (z. B. blockierende Anzeigen), ist nicht erlaubt.
   - Anzeigen, die die normale Verwendung der App oder den Spielverlauf beeinträchtigen, müssen sich nach 5 Sekunden schließen lassen – dies gilt auch für Anzeigen mit Prämie und von Nutzern aktivierte Werbung.
   - Mehrere Anzeigen-Placements auf einer Seite sind nicht zulässig. Beispiel: Banneranzeigen, die mehrere Angebote in einem Placement enthalten, oder mehrere Banner- oder Videoanzeigen.
   - Werbung muss eindeutig von App-Inhalten unterscheidbar sein.
   - Werbung darf keine schockierenden Inhalte zeigen oder emotional manipulativ wirken, um die Nutzer dazu zu verleiten, Anzeigen aufzurufen.
3. **Interessenbezogene Werbung/Remarketing**: Werbung, die minderjährigen Nutzern präsentiert wird, darf weder interessenbezogen sein (Werbung, die basierend auf ihrem Online-Browserverhalten auf einzelne Nutzer mit bestimmten Eigenschaften ausgerichtet ist) noch Remarketing (Werbung, die basierend auf vorherigen Interaktionen mit einer App oder Website auf einzelne Nutzer ausgerichtet ist) beinhalten.
4. **Datennutzung**: Sie (der SDK-Anbieter) müssen transparent darlegen, wie Sie mit Nutzerdaten umgehen (z. B. mit von einem Nutzer oder über einen Nutzer erhobenen Informationen, z. B. Geräteinformationen). Das bedeutet, den Zugriff auf die Daten sowie deren Erhebung, Verwendung und Weitergabe durch Ihr SDK offenzulegen und die Nutzung der Daten auf die angegebenen Zwecke zu beschränken. Die Google Play-Anforderungen gelten zusätzlich zu den Anforderungen der anwendbaren Datenschutzgesetze. Sie müssen die Erhebung jeglicher personenbezogener Daten und vertraulicher Informationen von Kindern durch Ihre App offenlegen, einschließlich, aber nicht beschränkt auf Authentifizierungsinformationen, Daten von Mikrofon- und Kamerasensoren, Geräte- und Werbenutzungsdaten sowie die Android-ID.
   - Sie müssen Entwicklern ermöglichen, entweder bei jeder Anfrage oder für jede App, eine auf Kinder ausgerichtete Anzeigenbereitstellung zu beantragen. Dabei müssen anwendbare Gesetze

und Bestimmungen, wie das US-Gesetz zum Schutz der Privatsphäre von Kindern im Internet (Children's Online Privacy Protection Act, COPPA) und die EU-Datenschutz-Grundverordnung (DSGVO) , eingehalten werden.

- Für Google Play müssen Anbieter von Anzeigen-SDKs bei allen Inhalten für Kinder personalisierte Werbeanzeigen, interessenbezogene Werbung und Remarketing deaktivieren.

- Wenn Sie Echtzeitgebote zur Auslieferung von Werbeanzeigen an Kinder verwenden, müssen die Datenschutzrichtlinien von den Bietern beachtet werden.
- Sie dürfen keine AAID, SIM-Seriennummer, Build-Seriennummer, BSSID, MAC-Adresse, SSID, IMEI und/oder IMSI von Kindern oder Nutzern unbekannten Alters übertragen.

5. **Vermittlungsplattformen**: Wenn Sie Kindern Werbung präsentieren, müssen Sie Folgendes beachten:
   - Nutzen Sie ausschließlich selbstzertifizierte Anzeigen-SDKs für familienfreundliche Inhalte oder implementieren Sie bestimmte Sicherheitsmaßnahmen, damit diese Anforderungen bei allen Werbeanzeigen, die durch Vermittlung ausgeliefert werden, befolgt werden.
   - Leiten Sie die erforderlichen Informationen an die Vermittlungsplattformen weiter, um diese über die Altersfreigabe für Anzeigeninhalte und etwaige Inhalte für Kinder in Kenntnis zu setzen.
6. **Selbstzertifizierung und Compliance**: Sie müssen genügend Informationen zur Verfügung stellen, z. B. über das Antragsformular , damit Google die Einhaltung aller Anforderungen an die Selbstzertifizierung seitens des Anzeigen-SDK bestätigen kann. Diese Informationen sind einschließlich, aber nicht beschränkt auf:
   - Eine englischsprachige Version der Nutzungsbedingungen, der Datenschutzerklärung und des Integrationsleitfadens für Publisher für Ihr SDK oder Ihre Vermittlungsplattform.
   - Eine Test-App , die die aktuelle konforme Version des Anzeigen-SDK nutzt. Sie muss als vollständiges und ausführbares Android-APK eingereicht werden, das alle Funktionen des SDKs nutzt. Anforderungen an Test-Apps:
     - Sie müssen als vollständiges und ausführbares Android-APK eingereicht werden, das auf einem Smartphone ausgeführt werden soll.
     - Sie müssen die aktuelle oder anstehende Version des Anzeigen-SDKs verwenden, die den Google Play-Richtlinien entspricht.
     - Sie müssen alle Funktionen Ihres Anzeigen-SDKs nutzen, etwa Ihr SDK aufrufen, um Anzeigen abzurufen und anzuzeigen.
     - Sie müssen uneingeschränkten Zugriff auf alle aktiven/ausgelieferten Anzeigeninventare im Netzwerk haben. Dies geschieht über die Anforderung von Creatives durch die Test-App.
     - Sie dürfen nicht per Standortbestimmung eingeschränkt werden.
     - Wenn Ihr Inventar für eine gemischte Zielgruppe bestimmt ist, muss Ihre Test-App zwischen Anfragen für Anzeigen-Creatives aus dem gesamten Inventar und dem Inventar für Kinder oder alle Altersgruppen unterscheiden können.
     - Sie dürfen nicht auf bestimmte Anzeigen im Inventar beschränkt sein, außer dies wird durch eine neutrale Altersabfrage gesteuert.
7. Sie müssen zeitnah auf mögliche Nachfragen reagieren und per Selbstzertifizierung bestätigen, dass bei alle neuen Versionen die aktuellen Google Play-Programmrichtlinien für Entwickler sowie die Anforderungen der Richtlinie für familienfreundliche Inhalte befolgt werden.
8. **Einhaltung gesetzlicher Bestimmungen**: Selbstzertifizierte Anzeigen-SDKs für familienfreundliche Inhalte müssen eine Anzeigenbereitstellung unterstützen, die alle relevanten Jugendschutzgesetze und -bestimmungen befolgt, die für die Publisher gelten.
   - Ihr SDK oder Ihre Vermittlungsplattform darf nicht gegen das US-Gesetz zum Schutz der Privatsphäre von Kindern im Internet (Children's Online Privacy Protection Act, COPPA) , die EU-Datenschutz-Grundverordnung (DSGVO) oder sonstige anwendbare Gesetze oder Bestimmungen verstoßen.

   Hinweis: Das Wort „Kinder“ kann in unterschiedlichen Sprachen und unterschiedlichen

Zusammenhängen verschiedene Bedeutungen haben. Es ist wichtig, dass Sie sich von Ihrem Rechtsbeistand dahingehend beraten lassen, welche Verpflichtungen und/oder altersbedingten Einschränkungen für Ihre App gelten. Sie selbst wissen am besten, wie Ihre App funktioniert. Deshalb benötigen wir Ihre Unterstützung, um dafür sorgen zu können, dass Familien Apps bei Google Play mit ruhigem Gewissen verwenden können.

Weitere Informationen zu diesen Anforderungen erhalten Sie auf der Richtlinienseite zum Programm für selbstzertifizierte Anzeigen-SDKs für familienfreundliche Inhalte .

Durchsetzung von Richtlinien

Richtlinienverstöße sollten natürlich am besten vermieden werden. Falls es aber doch einmal dazu kommen sollte, möchten wir dafür sorgen, dass Entwickler wissen, wie sie den Verstoß beheben können. Bitte teilen Sie uns mit, wenn Sie Verstöße feststellen oder Fragen zum Verwalten von Verstößen haben.

Anwendungsbereich von Richtlinien

Unsere Richtlinien gelten für alle Inhalte, die in Ihrer App angezeigt werden oder auf die sie verweist. Hierzu gehören auch jegliche dem Nutzer gezeigte Werbung und alle von Nutzern erstellten Inhalte, die von Ihrer App gehostet werden oder mit ihr verknüpft sind. Darüber hinaus gelten die Richtlinien für sämtliche Inhalte in Ihrem Entwicklerkonto, die bei Google Play öffentlich zugänglich sind, darunter Ihren Entwicklernamen sowie die Landingpage Ihrer aufgeführten Entwicklerwebsite.

Apps, mit denen Nutzer andere Apps auf ihren Geräten installieren können, sind nicht zulässig. Bei Apps, die ohne Installation Zugriff auf andere Apps, Spiele oder Software bieten, einschließlich Funktionen von Drittanbietern, muss gewährleistet sein, dass alle Inhalte, auf die sie Zugriff gewähren, allen Google Play-Richtlinien entsprechen. Außerdem können sie zusätzlichen Richtlinienüberprüfungen unterzogen werden.

Die in diesen Richtlinien verwendeten Begriffe haben die gleiche Bedeutung, wie sie jeweils für die Begriffe in der Vertriebsvereinbarung für Entwickler definiert ist. Der Inhalt Ihrer App muss nicht nur diesen Richtlinien und der Vertriebsvereinbarung für Entwickler entsprechen, sondern auch gemäß unseren Richtlinien zur Altersfreigabe bewertet werden.

Apps oder App-Inhalte, die das Vertrauen der Nutzer in Google Play untergraben, sind nicht zulässig. Bei der Beurteilung, ob Apps bei Google Play aufgenommen oder entfernt werden, berücksichtigen wir unter anderem, ob ein Muster für schädliches Verhalten oder ein hohes Missbrauchsrisiko vorliegt. Das Missbrauchsrisiko ermitteln wir unter anderem anhand verschiedener Aspekte wie App- oder entwicklerspezifischen Beschwerden, Nachrichten, früheren Verstößen, Feedback von Nutzern sowie Verwendung beliebter Marken, Figuren und anderer Assets.

Funktionsweise von Google Play Protect

Google Play Protect prüft Apps, während Sie diese installieren. Außerdem untersucht es regelmäßig Ihr Gerät. Wenn Play Protect eine potenziell schädliche App findet, sind folgende Szenarien möglich:

- Sie erhalten eine Benachrichtigung. Wenn die App entfernt werden soll, tippen Sie auf die Benachrichtigung und dann auf "Deinstallieren".
- Die App wird deaktiviert, bis Sie sie deinstallieren.
- Die App wird automatisch entfernt. In den meisten Fällen erhalten Sie eine Benachrichtigung, dass eine schädliche App entfernt wurde.

Funktionsweise des Malware-Schutzes

Damit Sie vor schädlicher Drittanbieter-Software, schädlichen URLs und anderen Sicherheitsproblemen geschützt sind, empfängt Google unter Umständen Informationen zu

- Netzwerkverbindungen des Geräts
- potenziell schädliche URLs
- Betriebssystem und Apps, die über Google Play oder andere Quellen auf Ihrem Gerät installiert wurden.

Sie erhalten ggf. eine Warnung von Google zu einer potenziell unsicheren App oder URL. Sollte die App bekanntermaßen schädlich für Geräte, Daten oder Nutzer sein, kann Google sie auch entfernen oder ihre Installation auf Ihrem Gerät blockieren.

Sie können einige dieser Schutzmechanismen in den Einstellungen auf Ihrem Gerät deaktivieren. Google kann jedoch weiterhin Informationen zu Apps erhalten, die über Google Play installiert wurden. Außerdem werden Apps, die über andere Quellen auf Ihrem Gerät installiert wurden, eventuell weiterhin auf Sicherheitsprobleme geprüft, ohne dass Informationen an Google gesendet werden.

Funktionsweise von Datenschutzwarnungen

Sie werden von Google Play Protect benachrichtigt, wenn eine App aus dem Google Play Store entfernt wird, weil sie möglicherweise auf Ihre personenbezogenen Daten zugreift. Sie haben dann die Möglichkeit, die App zu deinstallieren.

Durchsetzung

Sollte Ihre App oder Ihr Entwicklerkonto gegen eine unserer Richtlinien verstoßen, werden wir die unten aufgeführten Maßnahmen ergreifen. Darüber hinaus senden wir Ihnen per E-Mail relevante Informationen über die von uns ergriffenen Maßnahmen sowie eine Anleitung, wie Sie Einspruch erheben können, wenn Sie der Ansicht sind, dass wir die Maßnahmen irrtümlich ergriffen haben.

Beachten Sie, dass in Mitteilungen bezüglich Entfernungen oder in administrativen Mitteilungen möglicherweise nicht alle in Ihrem Konto, Ihrer App oder Ihrem App-Katalog vorhandenen Richtlinienverstöße aufgeführt sind. Es liegt in der Verantwortung der Entwickler, alle Richtlinienverstöße zu beseitigen und sorgfältig zu prüfen, ob die restlichen Apps oder das Konto den Richtlinien entspricht. Wenn Sie Richtlinienverstöße nicht in Ihrem Konto und allen Ihren Apps beheben, können zusätzliche Maßnahmen ergriffen werden.

Wiederholte oder schwerwiegende Verstöße gegen diese Richtlinien oder die Vertriebsvereinbarung für Entwickler , etwa im Falle von Malware, Betrug oder Apps, die Nutzern oder Geräten möglicherweise schaden, haben die Kündigung einzelner oder zugehöriger Google Play-Entwicklerkonten zur Folge.

Durchsetzungsmaßnahmen

Unterschiedliche Maßnahmen können unterschiedliche Auswirkungen auf Ihre Apps haben. Mithilfe einer Kombination aus automatischen und manuellen Mechanismen prüfen wir Apps und App-Inhalte, um Inhalte zu erkennen und zu bewerten, die gegen unsere Richtlinien verstoßen und schädlich für Nutzer und die Google Play-Plattform insgesamt sind. Mithilfe automatischer Modelle können wir mehr Verstöße erkennen und potenzielle Gefahren schneller bewerten, wodurch Google Play für alle sicherer ist. Inhalte, die gegen Richtlinien verstoßen, werden entweder von unseren automatischen Modellen entfernt oder – wenn eine differenziertere Einschätzung erforderlich ist – gekennzeichnet. Gekennzeichnete Inhalte werden dann von geschulten Mitarbeitern und Analysten weiter geprüft, z. B. weil es wichtig ist, den Kontext des Inhalts zu verstehen. Mit den Ergebnissen aus diesen manuellen Prüfungen werden dann unsere Modelle für maschinelles Lernen weiter optimiert.

Im folgenden Abschnitt werden die verschiedenen Maßnahmen, die Google Play ergreifen kann, sowie die Auswirkungen auf Ihre App und/oder Ihr Google Play-Entwicklerkonto beschrieben.

Sofern in einer Mitteilung zur Durchsetzung nicht anders angegeben, betreffen diese Maßnahmen alle Regionen. Wenn Ihre App zum Beispiel gesperrt wird, ist sie in keiner Region mehr verfügbar. Sofern

nicht anders angegeben, bleiben diese Maßnahmen in Kraft, es sei denn, Sie erheben gegen sie Einspruch und diesem wird stattgegeben.

Ablehnung

- Neue Apps oder App-Updates, die zur Überprüfung eingereicht werden, werden nicht bei Google Play verfügbar gemacht.
- Wenn ein Update zu einer vorhandenen App abgelehnt wurde, bleibt die vor dem Update veröffentlichte Version weiterhin bei Google Play verfügbar.
- Ablehnungen wirken sich nicht auf Ihren Zugriff auf vorhandene Installationen, Statistiken und Bewertungen einer abgelehnten App aus.
- Ablehnungen haben keine Auswirkungen auf den Status Ihres Google Play-Entwicklerkontos.

Hinweis: Versuchen Sie nicht, eine abgelehnte App noch einmal einzureichen, bevor Sie nicht alle Richtlinienverstöße behoben haben.

Entfernung

- Die App und alle vorherigen Versionen dieser App werden aus Google Play entfernt und können nicht mehr heruntergeladen werden.
- Da die App entfernt wird, können Nutzer ihren Store-Eintrag nicht mehr sehen. Diese Informationen werden wiederhergestellt, sobald Sie ein richtlinienkonformes Update der entfernten App einreichen.
- Nutzer können erst dann In-App-Käufe tätigen oder In-App-Abrechnungsfunktionen nutzen, wenn eine richtlinienkonforme Version der App von Google Play genehmigt wurde.
- Entfernungen wirken sich nicht sofort auf den Status Ihres Google Play-Entwicklerkontos aus. Mehrere Entfernungen können jedoch zu einer Sperrung führen.

Hinweis: Versuchen Sie nicht, eine entfernte App noch einmal zu veröffentlichen, bevor Sie nicht alle Richtlinienverstöße behoben haben.

Sperrung

- Die App und alle vorherigen Versionen dieser App werden aus Google Play entfernt und können nicht mehr heruntergeladen werden.
- Eine Sperrung kann sowohl aufgrund schwerwiegender oder mehrfacher Richtlinienverstöße als auch aufgrund wiederholter Ablehnungen oder Entfernungen von Apps erfolgen.
- Da die App gesperrt wird, können Nutzer ihren Store-Eintrag nicht mehr sehen. Diese Informationen werden wiederhergestellt, sobald Sie ein richtlinienkonformes Update einreichen.
- Sie können das APK oder App-Bundle einer gesperrten App nicht mehr verwenden.
- Nutzer können erst dann In-App-Käufe tätigen oder In-App-Abrechnungsfunktionen nutzen, wenn eine richtlinienkonforme Version der App von Google Play genehmigt wurde.
- Sperrungen werden als Verwarnungen gegen Ihr Google Play-Entwicklerkonto angesehen, sodass es nicht mehr als einwandfrei gilt. Mehrfache Verwarnungen können zur Kündigung einzelner und zugehöriger Google Play-Entwicklerkonten führen.

Hinweis: Versuchen Sie nicht, eine gesperrte App noch einmal zu veröffentlichen, es sei denn, Google Play hat Ihnen mitgeteilt, dass Sie dies tun dürfen.

Eingeschränkte Sichtbarkeit

- Die Sichtbarkeit Ihrer App bei Google Play ist eingeschränkt. Ihre App bleibt bei Google Play verfügbar und kann von Nutzern über einen direkten Link zum Play Store-Eintrag der App aufgerufen werden.

- Wenn Ihre App in den Status „Eingeschränkte Sichtbarkeit“ versetzt wurde, hat dies keine Auswirkungen auf den Status Ihres Google Play-Entwicklerkontos.
- Diese Maßnahme hat auch keinen Einfluss darauf, ob Nutzer den vorhandenen Store-Eintrag sehen können.

Eingeschränkte Regionen

- Ihre App kann über Google Play nur von Nutzern aus bestimmten Regionen heruntergeladen werden.
- Nutzer aus anderen Regionen können die App nicht im Play Store finden.
- Nutzer, die die App bereits installiert haben, können sie weiterhin auf ihren Geräten verwenden, erhalten aber keine Updates mehr.
- Die Beschränkung der Region hat keine Auswirkungen auf den Status Ihres Google Play-Entwicklerkontos.

Eingeschränktes Konto

- Wenn Ihr Entwicklerkonto eingeschränkt wird, werden alle Apps in Ihrem Katalog aus Google Play entfernt und Sie können keine neuen Apps mehr veröffentlichen und bestehende Apps nicht noch einmal veröffentlichen. Sie haben dann immer noch Zugriff auf die Play Console.
- Da alle Apps entfernt werden, können Nutzer die Store-Einträge dieser Apps und Ihr Entwicklerprofil nicht mehr sehen.
- Ihre aktuellen Nutzer können keine In-App-Käufe mehr tätigen und die In-App-Abrechnungsfunktionen Ihrer Apps nicht mehr nutzen.
- Sie können die Play Console weiterhin verwenden, um Google Play mehr Informationen zur Verfügung zu stellen und Ihre Kontoinformationen zu ändern.
- Sobald Sie alle Richtlinienverstöße behoben haben, können Sie Ihre Apps wieder veröffentlichen.

Kontokündigung

- Wenn Ihr Entwicklerkonto gekündigt wird, werden alle Apps in Ihrem Katalog aus Google Play entfernt und Sie können keine neuen Apps mehr veröffentlichen. Dies bedeutet auch, dass alle zugehörigen Google Play-Entwicklerkonten dauerhaft gesperrt werden.
- Mehrfache Sperrungen oder Sperrungen aufgrund schwerwiegender Richtlinienverstöße können auch die Kündigung Ihres Play Console-Kontos zur Folge haben.
- Da die Apps des gekündigten Kontos entfernt werden, können Nutzer die Store-Einträge dieser Apps und Ihr Entwicklerprofil nicht mehr sehen.
- Ihre aktuellen Nutzer können keine In-App-Käufe mehr tätigen und die In-App-Abrechnungsfunktionen Ihrer Apps nicht mehr nutzen.

Hinweis: Jedes neue Konto, das Sie zu eröffnen versuchen, wird ebenfalls gekündigt (ohne Erstattung der Registrierungsgebühr für Entwickler). Versuchen Sie daher nicht, sich für ein neues Play Console-Konto zu registrieren, während eines Ihrer anderen Konten gekündigt ist.

Inaktive Konten

Inaktive Konten sind Entwicklerkonten, die zeitweilig oder permanent nicht mehr verwendet werden. Sie gelten gemäß der Vertriebsvereinbarung für Entwickler nicht als einwandfrei.

Google Play-Entwicklerkonten sind für aktive Entwickler gedacht, die Apps veröffentlichen und aktualisieren. Zur Vermeidung von Missbrauch schließen wir Konten, die inaktiv sind oder nicht regelmäßig verwendet werden, um Apps zu veröffentlichen oder zu aktualisieren, Statistiken abzurufen oder Store-Einträge zu verwalten.

Bei der Kontoschließung werden das betreffende Konto und alle damit verbundenen Daten gelöscht. Die Registrierungsgebühr kann dabei nicht erstattet werden. Bevor wir Ihr inaktives Konto schließen,

werden wir Sie über die Kontaktdaten, die Sie für das Konto angegeben haben, über diesen Schritt informieren.

Wenn wir ein inaktives Konto schließen, können Sie trotzdem später ein neues Konto erstellen, um Spiele und Apps bei Google Play zu veröffentlichen. Sie können Ihr Konto nicht wieder aktivieren und Apps und Daten lassen sich nicht in ein neues Konto übertragen.

Richtlinienverstöße verwalten und melden

Einspruch gegen eine Maßnahme erheben

Apps werden im Play Store reaktiviert, wenn ein Fehler vorlag und wir feststellen, dass Ihre App nicht gegen die Google Play-Programmrichtlinien und die Vertriebsvereinbarung für Entwickler verstößt. Wenn Sie die Richtlinien sorgfältig gelesen haben und der Ansicht sind, dass unsere Entscheidung zu Unrecht erfolgt ist, folgen Sie der Anleitung in der E-Mail-Benachrichtigung über die Maßnahme oder klicken Sie hier, um Einspruch einzulegen.

Zusätzliche Ressourcen

Sollten Sie weitere Informationen zu einer Maßnahme oder einer Bewertung bzw. einem Kommentar eines Nutzers benötigen, sehen Sie sich die folgenden Hilfeartikel an oder kontaktieren Sie uns über die Google Play-Hilfe. Wir können Ihnen jedoch keine Rechtsberatung bieten. In diesem Fall sollten Sie sich an Ihren Rechtsbeistand wenden.

- App-Überprüfung
- Richtlinienverstoß melden
- Kontakt zu Kontokündigung oder App-Entfernung
- Faire Warnung
- Unangemessene Rezensionen
- Meine App wurde entfernt
- Kündigung von Entwicklerkonten

Vorgaben zur Nutzung der Play Console

Google Play möchte die Nutzung von Apps so sicher und angenehm wie möglich gestalten und allen Entwicklern optimale Geschäftschancen bieten. Im Zuge dessen soll auch die Bereitstellung Ihrer App möglichst reibungslos verlaufen.

Damit häufig auftretende Verstöße vermieden werden, sollten Sie die nachfolgenden Punkte beachten, wenn Sie Informationen über die Play Console und über Profile senden, die mit Ihrem Play Console-Entwicklerkonto verknüpft sind.

Folgende Voraussetzungen müssen erfüllt sein, bevor Sie Ihre App einreichen:

- Alle Informationen zum Entwicklerkonto wurden richtig angegeben, darunter:
  - Rechtsgültiger Name und Adresse
  - D-U-N-S-Nummer (bei der Registrierung als Organisation)
  - E-Mail-Adresse und Telefonnummer der Kontaktperson
  - E-Mail-Adresse und Telefonnummer des Entwicklers, die auf Google Play angezeigt werden (sofern zutreffend)
  - Zahlungsmethoden (sofern zutreffend)
  - Google-Zahlungsprofil, das mit Ihrem Entwicklerkonto verknüpft ist
- Bei der Registrierung als Organisation müssen Sie sicherstellen, dass die Informationen Ihres Entwicklerkontos auf dem neuesten Stand sind und mit den in ihrem Dun & Bradstreet-Profil

gespeicherten Angaben übereinstimmen.

- Alle App-Informationen und -Metadaten wurden korrekt angegeben.
- Sie haben die Datenschutzerklärung Ihrer App hochgeladen und alle erforderlichen Angaben im Abschnitt zur Datensicherheit gemacht.
- Sie haben ein aktives Demokonto, Anmeldeinformationen und alle weiteren Ressourcen angegeben, die zur Überprüfung Ihrer App erforderlich sind, z. B. Anmeldedaten oder einen QR-Code.

Wie immer gilt: Sorgen Sie für eine stabile, interaktive und responsive Nutzererfahrung und prüfen Sie, ob Ihre App, einschließlich Werbenetzwerken, Analysediensten und Drittanbieter-SDKs, den Google Play-Programmrichtlinien für Entwickler entspricht. Falls auch Kinder zu Ihrer Zielgruppe gehören, müssen Sie außerdem die Richtlinie für familienfreundliche Inhalte beachten.

Noch einmal zur Erinnerung: Sie müssen sich mit der Vertriebsvereinbarung für Entwickler sowie sämtlichen Programmrichtlinien für Entwickler vertraut machen und dafür sorgen, dass Ihre App alle Vorgaben erfüllt.

Developer Distribution Agreement

Benötigen Sie weitere Hilfe?

Mögliche weitere Schritte:

Kontakt

Weitere Informationen angeben und Hilfe erhalten