

Programmrichtlinien für Entwickler

(gültig ab 1. September 2021, 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 [Vereinbarung für den Entwicklervertrieb](#) 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 entweder unten oder als [Druckversion](#) 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 mit Inhalten, in denen Minderjährige sexualisiert werden, werden umgehend aus dem Store entfernt. Dazu gehören Apps, die Pädophilie oder unangemessene Interaktionen fördern, die auf Minderjährige ausgerichtet sind (z. B. Grapschen oder Streicheln).

Außerdem sind Apps verboten, die auf Kinder ausgerichtet sind, aber nicht jugendfreie Themen enthalten. Dazu gehören unter anderem Apps mit übermäßiger Darstellung von Gewalt und Blutvergießen und 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.

Sollten wir Kenntnis von Darstellungen des sexuellen Missbrauchs von Kindern erlangen, melden wir dies den zuständigen Behörden und löschen die Google-Konten der Personen, die mit der Verbreitung in Verbindung stehen.

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

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. Inhalte, in denen Nacktheit offen dargestellt wird, sind erlaubt, wenn sie hauptsächlich pädagogischen, dokumentarischen, wissenschaftlichen oder künstlerischen Zwecken dienen und nicht überflüssig sind.

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 unbedeckt, weichgezeichnet oder nur minimal bedeckt 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 darstellen oder die funktional sexuelle Hilfsmittel sind, Sexanleitungen, illegale sexuelle Themen und Fetische
- 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 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

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 oder ähnlichen Eigenschaften, die mit systematischer Diskriminierung oder Ausgrenzung verbunden sind, aufgerufen wird, 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 Hintergrundinformationen zu liefern, sodass andere Nutzer den Zusammenhang verstehen.

Sensible Ereignisse

Apps, die aus Naturkatastrophen, Gräueltaten, Gesundheitskrisen, Konflikten, Todesfällen oder anderen tragischen Ereignissen einen Nutzen zu ziehen versuchen oder in solchen Fällen mangelnde Sensibilität aufweisen, 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 bedeutenden tragischen Ereignisses

- Profitieren von einem tragischen 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.

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

- Darstellung bzw. Förderung des Konsums oder Verkaufs von Alkohol oder Tabak an Minderjährige
- Andeutung, dass sich der Konsum von Tabak positiv auf die gesellschaftliche, sexuelle, berufliche, intellektuelle oder sportliche Stellung auswirkt
- Vorteilhafte Darstellung von übermäßigem Alkoholkonsum, einschließlich der positiven Darstellung von übermäßigem Alkoholkonsum, Trinkgelagen oder Trinkwettbewerben

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 Bestimmungen und diejenigen auf Landesebene für alle Regionen oder Länder einhalten, auf die Ihre App ausgerichtet ist. So kann es

gemäß der örtlichen Gesetzgebung beispielsweise erforderlich sein, bestimmte Informationen offenzulegen.

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

Gültig ab 15. September 2021

Wir definieren einen Privatkredit als ein einmaliges Darlehen, das eine Einzelperson, ein Unternehmen oder eine Rechtspersönlichkeit 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, Rückzahlungszeitplan, 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, revolvingierende 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.

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, die Kredite direkt anbieten, für Lead-Generatoren und für Apps, die direkten Kontakt zwischen Kunden und als Kreditgeber fungierenden Drittparteien herstellen.

Für Indien und Indonesien geltende zusätzliche Anforderungen für Apps, die Privatkredite anbieten

In Indien und Indonesien müssen Apps für Privatkredite anhand der unten stehenden zusätzlichen Nachweise belegen, dass die geforderten Voraussetzungen erfüllt sind.

1. Indien

- [Füllen Sie die für Indien erforderliche Erklärung für Apps aus, die Privatkredite anbieten](#), und legen Sie die erforderlichen Unterlagen bei, die Ihre Erklärung stützen. Beispiel:
 - 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 oder Banken leihen können, müssen Sie dies in der Erklärung genau angeben.
- Achten Sie darauf, dass der Name des zugehörigen registrierten Unternehmens, der in Ihrer Erklärung angegeben ist, im Namen des Entwicklerkontos enthalten ist.

2. Indonesien

- Es sind nur Apps für Privatkredite zulässig, die eine Lizenz der indonesischen Finanzaufsichtsbehörde (Otoritas Jasa Keuangan, OJK) haben oder dort registriert sind.
- [Füllen Sie die für Indonesien erforderliche Erklärung für Apps aus, die Privatkredite anbieten](#), und legen Sie die Unterlagen der OJK bei, die Ihre Erklärung stützen.
- Achten Sie darauf, dass der Name des zugehörigen registrierten Unternehmens, der in Ihrer Erklärung angegeben ist, im Namen des Entwicklerkontos enthalten 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.

< Back

Easy Loans
offers in app purchases

★ ★ ★ ★ ★ 1255

Install

Are you looking for a speedy loan?

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

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

Violations

- No minimum and maximum period for repayment
- Doesn't disclose Maximum Annual Percentage Rate (APR), which generally includes interest rate plus fees and other costs for a year, or similar other rate calculated consistently with local law
- No representative example of the total cost of the loan, including all applicable fees

Glücksspiele

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 den in der folgenden Tabelle aufgeführten 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 (in der unten stehenden Tabelle sind die genauen Arten von Glücksspielprodukten aufgeführt, die in den jeweiligen Ländern zulässig sind):

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

Zusammenfassung	Details
Mit Einschränkungen zulässig	Vorbehaltlich der im vorliegenden Abschnitt zu Glücksspiel-Apps genannten Antrags- und Zulassungsanforderungen sind Apps mit folgenden Arten von Glücksspielprodukten zulässig: <ul style="list-style-type: none"> • Sportwetten (einschließlich Daily Fantasy Sports, sofern gesetzlich erlaubt) • Lotterien

Belgien

Zusammenfassung	Details
Mit Einschränkungen zulässig	Vorbehaltlich der im vorliegenden Abschnitt zu Glücksspiel-Apps genannten Antrags- und Zulassungsanforderungen sind Apps mit folgenden Arten von Glücksspielprodukten zulässig: <ul style="list-style-type: none"> • Online-Casinospiele • Sportwetten • Lotterien (nur staatliche Betreiber)

Brasilien

Zusammenfassung	Details
Mit Einschränkungen zulässig	Vorbehaltlich der im vorliegenden Abschnitt zu Glücksspiel-Apps genannten Antrags- und Zulassungsanforderungen sind Apps mit folgenden Arten von Glücksspielprodukten zulässig: <ul style="list-style-type: none"> • Sportwetten (nur Pferderennen) • Lotterien (nur genehmigte und durch die Caixa Econômica Federal veröffentlichte Apps)

Kanada

Zusammenfassung	Details
Mit Einschränkungen zulässig	Vorbehaltlich der im vorliegenden Abschnitt zu Glücksspiel-Apps genannten Antrags- und Zulassungsanforderungen sind Apps mit folgenden Arten von Glücksspielprodukten zulässig: <ul style="list-style-type: none"> • Online-Casinospiele (nur staatliche Betreiber) • Sportwetten (nur staatliche Betreiber) • Lotterien (nur staatliche Betreiber)

Kolumbien

Zusammenfassung	Details
Mit Einschränkungen zulässig	Vorbehaltlich der im vorliegenden Abschnitt zu Glücksspiel-Apps genannten Antrags- und Zulassungsanforderungen sind Apps mit folgenden Arten von Glücksspielprodukten zulässig: <ul style="list-style-type: none"> • Online-Casinospiele • Sportwetten • Lotterien (nur staatliche Betreiber)

Dänemark

Zusammenfassung	Details
Mit Einschränkungen zulässig	Vorbehaltlich der im vorliegenden Abschnitt zu Glücksspiel-Apps genannten Antrags- und Zulassungsanforderungen sind Apps mit folgenden Arten von Glücksspielprodukten zulässig: <ul style="list-style-type: none"> • Online-Casinospiele • Sportwetten (einschließlich Daily Fantasy Sports, sofern gesetzlich erlaubt) • Lotterien

Finnland

Zusammenfassung	Details
Mit Einschränkungen zulässig	Vorbehaltlich der im vorliegenden Abschnitt zu Glücksspiel-Apps genannten Antrags- und Zulassungsanforderungen sind Apps mit folgenden Arten von Glücksspielprodukten zulässig: <ul style="list-style-type: none"> • Online-Casinospiele (nur staatliche Betreiber) • Sportwetten (nur staatliche Betreiber) • Lotterien (nur staatliche Betreiber)

Frankreich

Zusammenfassung	Details
Mit Einschränkungen zulässig	Vorbehaltlich der im vorliegenden Abschnitt zu Glücksspiel-Apps genannten Antrags- und Zulassungsanforderungen sind Apps mit folgenden Arten von Glücksspielprodukten zulässig: <ul style="list-style-type: none"> • Online-Casinospiele • Sportwetten • Pferderennen (sofern diese getrennt von Sportwetten reguliert und lizenziert sind) • Lotterien (nur staatliche Betreiber)

Deutschland

Zusammenfassung	Details
Mit Einschränkungen zulässig	Vorbehaltlich der im vorliegenden Abschnitt zu Glücksspiel-Apps genannten Antrags- und Zulassungsanforderungen sind Apps mit folgenden Arten von Glücksspielprodukten zulässig: <ul style="list-style-type: none"> • Sportwetten • Pferderennen (sofern diese getrennt von Sportwetten reguliert und lizenziert sind) • Lotterien (nur staatliche Betreiber oder von staatlichen Stellen beauftragte Anbieter)

Irland

Zusammenfassung	Details

Zusammenfassung	Details
Mit Einschränkungen zulässig	Vorbehaltlich der im vorliegenden Abschnitt zu Glücksspiel-Apps genannten Antrags- und Zulassungsanforderungen sind Apps mit folgenden Arten von Glücksspielprodukten zulässig: <ul style="list-style-type: none"> • Online-Casinospiele • Sportwetten • Lotterien (nur staatliche oder gemeinnützige Betreiber)

Japan

Zusammenfassung	Details
Mit Einschränkungen zulässig	Vorbehaltlich der im vorliegenden Abschnitt zu Glücksspiel-Apps genannten Antrags- und Zulassungsanforderungen sind Apps mit folgenden Arten von Glücksspielprodukten zulässig: <ul style="list-style-type: none"> • Sportwetten (Pferde-, Motorboot-, Fahrrad- und Motorradrennen sowie Fußballwetten – nur staatliche Betreiber) • Lotterien (nur staatliche Betreiber)

Mexiko

Zusammenfassung	Details
Mit Einschränkungen zulässig	Vorbehaltlich der im vorliegenden Abschnitt zu Glücksspiel-Apps genannten Antrags- und Zulassungsanforderungen sind Apps mit folgenden Arten von Glücksspielprodukten zulässig: <ul style="list-style-type: none"> • Online-Casinospiele • Sportwetten • Lotterien • Daily Fantasy Sports

Neuseeland

Zusammenfassung	Details
Mit Einschränkungen zulässig	Vorbehaltlich der im vorliegenden Abschnitt zu Glücksspiel-Apps genannten Antrags- und Zulassungsanforderungen sind Apps mit folgenden Arten von Glücksspielprodukten zulässig: <ul style="list-style-type: none"> • Sportwetten (nur staatliche Betreiber) • Lotterien (nur staatliche Betreiber)

Norwegen

Zusammenfassung	Details
Mit Einschränkungen zulässig	Vorbehaltlich der im vorliegenden Abschnitt zu Glücksspiel-Apps genannten Antrags- und Zulassungsanforderungen sind Apps mit folgenden Arten von Glücksspielprodukten zulässig: <ul style="list-style-type: none"> • Online-Casinospiele • Sportwetten (nur staatliche Betreiber) • Lotterien

Rumänien

Zusammenfassung	Details
Mit Einschränkungen zulässig	Vorbehaltlich der im vorliegenden Abschnitt zu Glücksspiel-Apps genannten Antrags- und Zulassungsanforderungen sind Apps mit folgenden Arten von Glücksspielprodukten zulässig: <ul style="list-style-type: none">• Online-Casinospiele• Sportwetten• Lotterien (nur staatliche Betreiber)

Spanien

Zusammenfassung	Details
Mit Einschränkungen zulässig	Vorbehaltlich der im vorliegenden Abschnitt zu Glücksspiel-Apps genannten Antrags- und Zulassungsanforderungen sind Apps mit folgenden Arten von Glücksspielprodukten zulässig: <ul style="list-style-type: none">• Online-Casinospiele• Sportwetten (einschließlich Daily Fantasy Sports, sofern gesetzlich erlaubt)• Pferderennen (sofern diese getrennt von Sportwetten reguliert und lizenziert sind)• Lotterien (nur staatliche Betreiber)

Schweden

Zusammenfassung	Details
Mit Einschränkungen zulässig	Vorbehaltlich der im vorliegenden Abschnitt zu Glücksspiel-Apps genannten Antrags- und Zulassungsanforderungen sind Apps mit folgenden Arten von Glücksspielprodukten zulässig: <ul style="list-style-type: none">• Online-Casinospiele• Sportwetten• Lotterien (nur staatliche Betreiber)

Vereinigtes Königreich

Zusammenfassung	Details
Mit Einschränkungen zulässig	Vorbehaltlich der im vorliegenden Abschnitt zu Glücksspiel-Apps genannten Antrags- und Zulassungsanforderungen sind Apps mit folgenden Arten von Glücksspielprodukten zulässig: <ul style="list-style-type: none">• Online-Casinospiele• Sportwetten (einschließlich Daily Fantasy Sports, sofern gesetzlich erlaubt)• Lotterien

USA

Zusammenfassung	Details
-----------------	---------

Zusammenfassung	Details
Mit Einschränkungen zulässig	<p>Vorbehaltlich der im vorliegenden Abschnitt zu Glücksspiel-Apps genannten Antrags- und Zulassungsanforderungen sind Apps mit folgenden Arten von Glücksspielprodukten in gewissen Bundesstaaten zulässig, sofern sie gesetzlich erlaubt und ordnungsgemäß lizenziert sind:</p> <ul style="list-style-type: none"> • Online-Casinospiele • Sportwetten • Pferderennen (sofern getrennt von Sportwetten reguliert und lizenziert) • Lotterien <p>Wenn ein Bundesstaat oder Glücksspielprodukt für einen Bundesstaat nicht auf dem Antragsformular vorhanden ist, gestattet Google Play derzeit keinen Vertrieb.</p> <p>Je nach Bundesstaat können Daily Fantasy Sports (DFS) in den Vereinigten Staaten als Glücksspiel betrachtet werden und alle in den Vereinigten Staaten veröffentlichten Daily-Fantasy-Sports-Apps unterliegen den nachstehenden Anforderungen an Daily-Fantasy-Sports-Apps.</p>

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 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, sind Inhalte oder Dienste unzulässig, die es Nutzern ermöglichen oder erleichtern, mit echtem Geld zu wetten, zu investieren oder teilzunehmen (einschließlich mit Geld gekaufter In-App-Artikel), 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 angeboten 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

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 Nutzungsbedingungen müssen die Wahrscheinlichkeiten oder die Auswahlmethode alle Treuepunkteprogramme mit Zufallsmechanismen offengelegt werden
Spiel	Nicht zulässig	Zulässig	Erforderlich	Nicht zutreffend (Spiele sind keine Zufallsmechanismen-Treuepunkteprogramme-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 Casinospiele, 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 oder verschreibungspflichtigen Medikamenten ohne Rezept
 - Darstellung des Konsums oder Verkaufs von Drogen, Alkohol oder Tabak 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 oder zugänglich sind.

Apps, die von Nutzern erstellte Inhalte enthalten oder darauf verweisen, müssen folgende Vorgaben erfüllen:

- Nutzer müssen die Nutzungsbedingungen und/oder Nutzerrichtlinien der App akzeptieren, bevor sie Inhalte erstellen oder hochladen dürfen.
- Anstößige 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 zuverlässige, wirksame und dauerhafte Verfahren zur Moderation der von Nutzern erstellten Inhalte implementiert werden, die den in der App gehosteten Inhalten gerecht werden.
 - Bei Livestreaming-Apps müssen unangemessene von Nutzern erstellte Inhalte so zeitnah wie möglich entfernt werden.
 - Bei Augmented Reality-Apps (AR) müssen bei der Moderation der von Nutzern erstellten Inhalte (einschließlich des In-App-Berichtssystems) sowohl anstößige 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 nutzerfreundliches System zum Melden unangemessener von Nutzern erstellter Inhalte umfassen und es müssen gegebenenfalls entsprechende Maßnahmen ergriffen werden.
- Sich unangemessen verhaltende Nutzer, die gegen die Nutzungsbedingungen und/oder Nutzerrichtlinien der App verstoßen, müssen entfernt oder blockiert werden.
- Es müssen Absicherungen implementiert werden, um zu vermeiden, dass unangemessenes Nutzerverhalten durch In-App-Monetarisierung gefördert wird.

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
-

Nicht freigegebene Substanzen

Google Play gestattet keine Apps, die nicht genehmigte Substanzen bewerben oder verkaufen. Behauptungen der Legalität werden dabei nicht berücksichtigt. Beispiele:

- 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 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.

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.

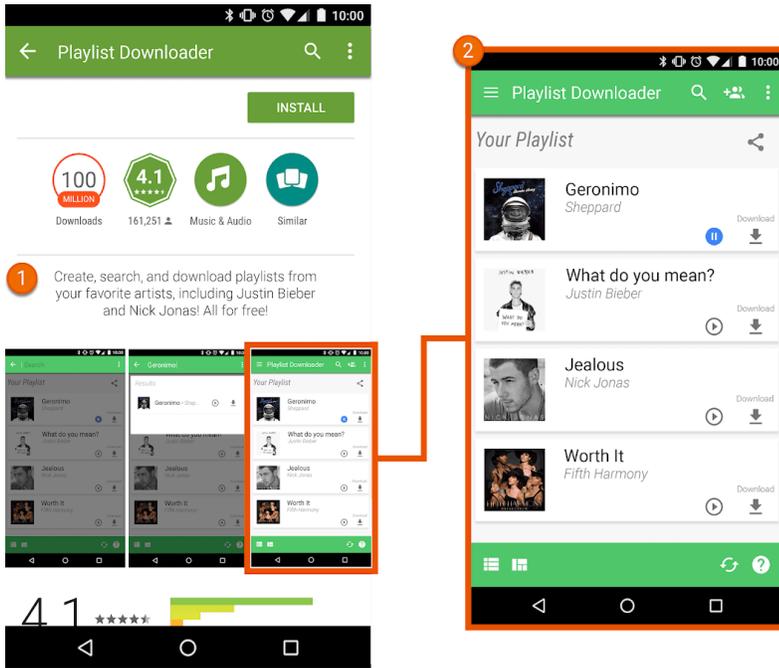
- Covergestaltung für Musikalben, Videospiele und Bücher
- Marketingbilder aus Filmen, Videospielen oder aus dem Fernsehen
- Grafiken oder Bilder aus Comicbüchern, Cartoons, Filmen, Musikvideos oder aus dem Fernsehen
- Logos von College- oder Profimannschaften
- Fotos aus dem Social Media-Konto einer 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, Sicherheit und Betrug

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. Dazu gehören beispielsweise vom Nutzer bereitgestellte Informationen und Informationen, die über einen Nutzer erfasst werden, einschließlich Geräteinformationen. Das bedeutet, dass Sie den Zugriff auf die Daten sowie deren Erhebung, Verwendung und Weitergabe offenlegen und die Nutzung der Daten auf die angegebenen Zwecke beschränken müssen. Falls in Ihrer App personenbezogene und vertrauliche Nutzerdaten verarbeitet werden, gelten zusätzlich die Anforderungen im Abschnitt „Personenbezogene und vertrauliche Daten“ weiter unten. Diese Google Play-Anforderungen gelten zusätzlich zu den Anforderungen der geltenden Datenschutzgesetze. Wenn Sie in Ihrer App Drittanbietercode verwenden, z. B. SDKs, müssen Sie gewährleisten, dass dieser den Programmrichtlinien für Entwickler entspricht.

Personenbezogene und vertrauliche Daten

Personenbezogene oder vertrauliche Nutzerdaten umfassen unter anderem personenidentifizierbare Informationen, Finanz- und Zahlungsinformationen, Authentifizierungsinformationen, Telefonbuchdaten, Kontakte, den [Gerätestandort](#), SMS- und anrufbezogene Daten, andere Apps auf dem Gerät, Mikrofon- und Kameradaten sowie andere vertrauliche Geräte- oder Nutzungsdaten. Wenn Ihre App personenbezogene oder vertrauliche Nutzerdaten verarbeitet, müssen Sie Folgendes tun:

- Sie müssen den Zugriff auf personenbezogene und vertrauliche Daten über die App sowie deren Erhebung, Verwendung und Weitergabe auf Zwecke beschränken, die in direktem Zusammenhang mit der Bereitstellung und Verbesserung der Funktionen der App stehen (z. B. vom Nutzer erwartete Funktionen, die in der Beschreibung der App bei Google Play dokumentiert sind und beworben werden). Die Weitergabe von personenbezogenen und vertraulichen Nutzerdaten beinhaltet auch die Verwendung von SDKs oder anderen Diensten Dritter, mit denen Daten an Dritte übertragen werden. Apps, in denen personenbezogene und vertrauliche Nutzerdaten außerdem zur Bereitstellung von Werbung verwendet werden, müssen unsere [Werberichtlinien](#) einhalten.
- 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 auf Daten zugreifen, die durch [Android-Berechtigungen](#) geschützt sind.
- Sie dürfen keine personenbezogenen und vertraulichen Nutzerdaten verkaufen.

Pflicht zur deutlichen Offenlegung und Zustimmung

Wenn Nutzer nicht in angemessener Weise davon ausgehen können, dass ihre personenbezogenen und vertraulichen Nutzerdaten zur Bereitstellung oder Verbesserung richtlinienkonformer Funktionen Ihrer App erforderlich sind (z. B. Datenerhebung im Hintergrund Ihrer App), müssen Sie Folgendes gewährleisten:

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.

Unmittelbar nach der Offenlegung innerhalb der App muss eine Anfrage zur Zustimmung des Nutzers und, sofern verfügbar, eine damit verknüpfte Laufzeitberechtigungsanfrage gestellt werden. Solange der Nutzer nicht zustimmt, dürfen Sie auf keinerlei personenbezogene und vertrauliche Daten zugreifen bzw. solche Daten erheben. 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 Zustimmung 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 Erlangen der Zustimmung des Nutzers verwendet 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, 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 die Nutzung entgegen den oben stehenden Anforderungen nicht umfassend offenlegen und eine Einwilligung dafür einholen
- Apps, die eingeschränkte Berechtigungen im Hintergrund erheben, einschließlich für Tracking-, Recherche- oder Marketingzwecke, und die Nutzung entgegen den oben stehenden Anforderungen nicht umfassend offenlegen und eine Einwilligung dafür einholen

Gültig ab 28. Oktober 2021:

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	<p>Gleichbleibende Geräte-IDs dürfen nicht mit anderen personenbezogenen und vertraulichen Nutzerdaten oder zurücksetzbaren Geräte-IDs verknüpft werden, mit folgenden Ausnahmen:</p> <ul style="list-style-type: none"> • 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-Eigentümergebiet <p>Diese Verwendungszwecke müssen für Nutzer entsprechend den Richtlinien zu Nutzerdaten deutlich sichtbar angebracht sein.</p> <p>In dieser Ressource finden Sie Informationen zu alternativen eindeutigen Kennzeichnungen.</p> <p>In der Werberichtlinie finden Sie zusätzliche Informationen zur Android-Werbe-ID.</p>

Abschnitt zur Datensicherheit

Gültig ab 1. April 2022

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

Datenschutzerklärung

Für alle Apps muss eine Datenschutzerklärung im dafür vorgesehenen Feld in der Play Console sowie in der App selbst veröffentlicht werden. In der Erklärung sowie in Bekanntmachungen 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:

- Entwicklerinformationen und einen Ansprechpartner bei Fragen zum Datenschutz oder eine Möglichkeit, Anfragen zu stellen
- Eine Beschreibung der Arten von personenbezogenen und vertraulichen Daten, 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

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

Ihre Datenschutzerklärung muss unter einer aktiven URL (keine PDF-Datei) verfügbar sein und darf nicht bearbeitbar sein.

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. AAdID) 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

Anfragen für Berechtigungen und APIs, die auf vertrauliche Informationen zugreifen, 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 offenbarte, nicht implementierte oder nicht zugelassene Funktionen oder Zwecke ermöglichen, dürfen nicht verwendet werden. Personenbezogene und sensible Daten, auf die über Berechtigungen oder APIs zugegriffen wird, dürfen niemals verkauft werden.

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:

- Sensible Nutzer- oder Gerätedaten, auf die mit eingeschränkten Berechtigungen zugegriffen wird, dürfen nur an Dritte weitergegeben werden, wenn das erforderlich ist, um vorhandene Funktionen oder Dienste innerhalb der App, aus der die Daten stammen, bereitzustellen oder zu verbessern. Die Weitergabe von Daten ist auch zulässig, soweit dies gemäß geltendem Recht oder im Rahmen einer Fusion, einer Übernahme oder eines Verkaufs von Vermögenswerten erforderlich ist. In diesem Fall müssen die Nutzer angemessen darüber informiert werden. Eine anderweitige Weitergabe oder ein Verkauf von Nutzerdaten ist untersagt.
- 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 sensible Berechtigungen verweigern, so weit wie möglich entgegenkommen. Wenn ein Nutzer z. B. den Zugriff auf die Anrufliste eingeschränkt hat, sollten Sie ihm die Möglichkeit geben, Telefonnummern manuell einzugeben.
- Die Verwendung von Berechtigungen entgegen den offiziellen [Best Practices für App-Berechtigungen für Android-Entwickler](#) und die Verletzung bestehender Richtlinien, insbesondere bezüglich des [Missbrauchs von erhöhten Berechtigungen](#), ist ausdrücklich 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](#) sowie den folgenden Einschränkungen unterliegen:

- Entwickler von 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 Analyse Zwecken 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

Effective October 15, 2021

Die Accessibility API darf für Folgendes nicht verwendet werden:

- Ändern von Nutzereinstellungen ohne Einwilligung des Nutzers, es sei denn, die Änderung wurde durch einen Elternteil oder Erziehungsberechtigten über eine Jugendschutz-App autorisiert oder von autorisierten Administratoren über eine Unternehmenssoftware vorgenommen
- Hindern der Nutzer, die App oder den Dienst zu deaktivieren oder zu deinstallieren
- 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 Nutzung der Accessibility API muss im Google Play-Eintrag dokumentiert sein.

Richtlinien für das `IsAccessibilityTool`

Apps, deren Hauptfunktionen Menschen mit Behinderung direkt unterstützen sollen, dürfen das Attribut `IsAccessibilityTool` nutzen, um sich offiziell als Bedienungshilfen-App auszuweisen.

Apps, für die die Verwendung des `IsAccessibilityTool` nicht vorgesehen ist, dürfen diese Bezeichnung nicht nutzen und 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 zur 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.

Missbrauch von Geräten und Netzwerken

Effective October 15, 2021

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 Mobilfunknetzbetreibers, 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.
-

Irreführendes Verhalten

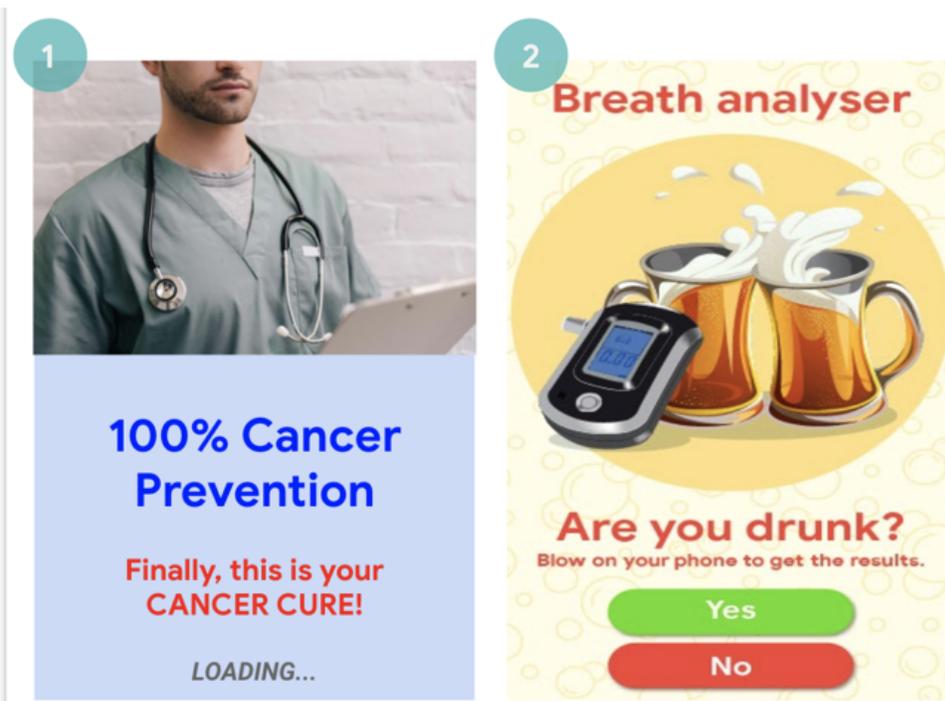
Apps, mit denen Nutzer getäuscht werden sollen oder die unlauteres Verhalten ermöglichen, sind nicht zulässig. Dazu gehören unter anderem Apps, die keine Funktion haben. Die Funktionalität von Apps muss in allen Teilen der Metadaten genau dargelegt, beschrieben und mit Bildern/Videos erläutert werden. 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 medizinischen oder gesundheitsbezogenen Inhalten oder Funktionen, die irreführend oder potenziell schädlich sind
- Apps mit angeblichen Funktionen, die in Wirklichkeit nicht realisierbar sind (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 gar 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, Abschlüsse, Kreditkarten und Führerscheine erstellt werden können bzw. die deren Erstellung ermöglichen. Die Funktionalität und/oder der Inhalt der App müssen genau dargelegt und durch Titel, Beschreibungen sowie Bilder/Videos erläutert werden und müssen 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 unsere Richtlinien erfüllen.

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 Rechtspersonlichkeiten 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.

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.
-

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 Anmeldeinformationen 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, über den personenbezogene oder vertrauliche Nutzerdaten von einem Gerät erfasst bzw. versendet werden, ohne den Nutzer ausreichend darüber zu informieren oder seine Zustimmung einzuholen und ohne einen dauerhaft sichtbaren Hinweis zu diesem Vorgang anzuzeigen.

Stalkerware-Apps zielen auf Nutzer ab, indem sie personenbezogene oder vertrauliche Nutzerdaten beobachten und diese Daten an Dritte versenden oder Dritten zugänglich machen.

Nur Apps, die ausschließlich für die Überwachung durch Eltern oder Unternehmensführungen entworfen und vermarktet werden, sind als Überwachungs-Apps zulässig, sofern sie die unten beschriebenen Anforderungen vollständig erfüllen. Diese Apps dürfen jedoch nicht verwendet werden, um Personen (z. B. einen Partner) ohne ihr Wissen oder ihre Zustimmung zu überwachen, unabhängig davon, ob ein dauerhaft sichtbarer Hinweis angezeigt wird.

Im Play Store vertriebene Apps, die keine Stalkerware sind, aber das Verhalten eines Nutzers auf einem Gerät überwachen oder verfolgen, müssen die folgenden Anforderungen erfüllen:

- Sie 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 sowie ein Symbol zur eindeutigen Identifikation der App eingeblendet werden, wenn sie ausgeführt wird.
- 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.
- Sie sind für die Rechtmäßigkeit Ihrer App im jeweiligen Zielland verantwortlich. Apps, die im Land der Veröffentlichung rechtswidrig sind, werden entfernt.

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 Rechtausweitung, 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 Nutzereinstimmung 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.

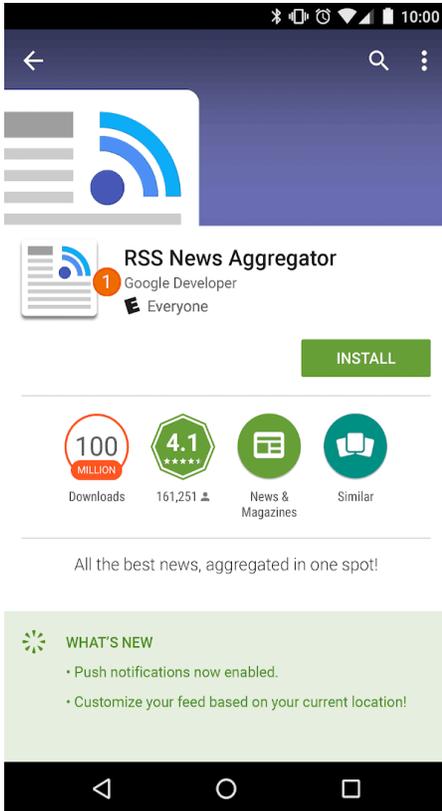
Wenn eine App jedoch die Ausführung von beliebigem Code erlaubt und kein Grund zur Annahme besteht, dass böswilliges Verhalten dahinter steckt, spricht man stattdessen von einer Sicherheitslücke, die der Entwickler mit einem Patch beheben muss.

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 fälschlicherweise eine Beziehung zu einem anderen Unternehmen oder Entwickler suggerieren:



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

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

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

- 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:

- Werbetbetrug
- 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
-

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.

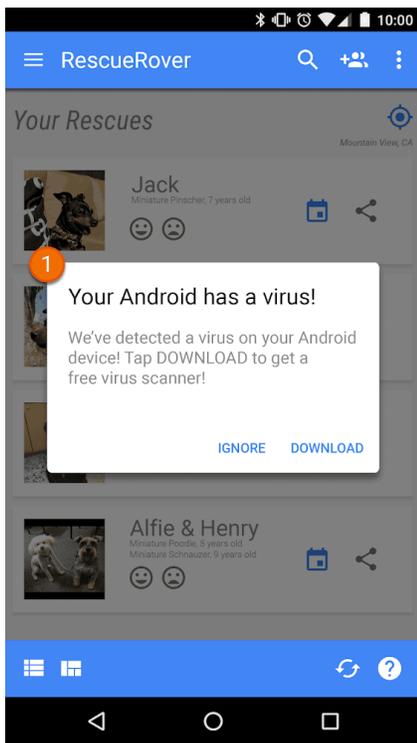
- Apps, die Anzeigen rendern, die für den Nutzer nicht sichtbar sind
 - Apps, die automatisch Klicks auf Anzeigen generieren, ohne dass der Nutzer dies beabsichtigt, oder entsprechenden Netzwerkverkehr erzeugen, um betrügerische Klick-Gutschriften zu erzeugen
 - Apps, die gefälschte Klicks zur Installationsattribution 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 Apps und Downloads bei Google Play in Rechnung stellen, müssen das Abrechnungssystem von Google Play als Zahlungsmethode verwenden.
2. Für Apps, die über Play vertrieben werden, muss das Abrechnungssystem von Google Play als Zahlungsmethode verwendet werden, wenn für den Zugriff auf Funktionen oder Dienste der App, einschließlich App-Funktionen, digitaler Inhalte oder Waren, eine Zahlung gefordert oder akzeptiert wird.
 - a. 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)
 - Abonnementdienste (z. B. Fitness-, Spiele-, Dating-, Bildungs-, Musik-, Video- und andere Inhaltsabos)
 - 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

b. Das Abrechnungssystem von Google Play darf in folgenden Fällen nicht verwendet werden:

- Die Zahlung erfolgt hauptsächlich:
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](#).
 - 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
 - Als Überweisung in Bezug auf eine Kreditkartenabrechnung oder eine Stromrechnung, beispielsweise Kabel- und Telekommunikationsdienste
- Zahlungen umfassen Peer-to-Peer-Zahlungen, Online-Auktionen und steuerbefreite Spenden.
- 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.
- Die Zahlung erfolgt für eine Produktkategorie, die gemäß den [Inhaltsrichtlinien des Zahlungscenters](#) von Google nicht akzeptiert wird.

3. Apps, die nicht unter 2(b) beschrieben sind, dürfen Nutzer nicht zu einer anderen Zahlungsmethode als dem Abrechnungssystem von Google Play weiterleiten. 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
- 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

4. Virtuelles In-App-Geld darf nur innerhalb der App oder des Spieltitels verwendet werden, in dem es ursprünglich erworben wurde.

5. 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.

6. 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.

Hinweis: [In unserer Hilfe](#) finden Sie Informationen zu Fristen und häufig gestellte Fragen bezüglich dieser Richtlinie.

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](#).

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](#).

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:

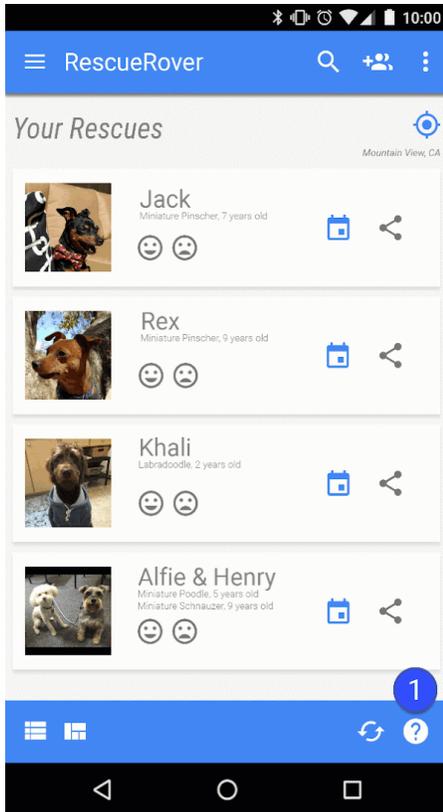
- Der Nutzer muss eindeutig darauf hingewiesen werden, dass die im Rahmen der Berechtigung angeforderten Daten zum Gerätestandort zu Werbezwecken verwendet oder erhoben werden. Außerdem muss dies in der verbindlichen Datenschutzerklärung der App dokumentiert sein, einschließlich Links zu relevanten Datenschutzerklärungen 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.

Irreführende Werbung

Werbeanzeigen dürfen weder die Benutzeroberfläche einer App noch Betriebssystembenachrichtigungen oder -warnungen simulieren oder nachahmen. Es muss für Nutzer eindeutig erkennbar sein, über welche App die Werbeanzeige geschaltet wird.

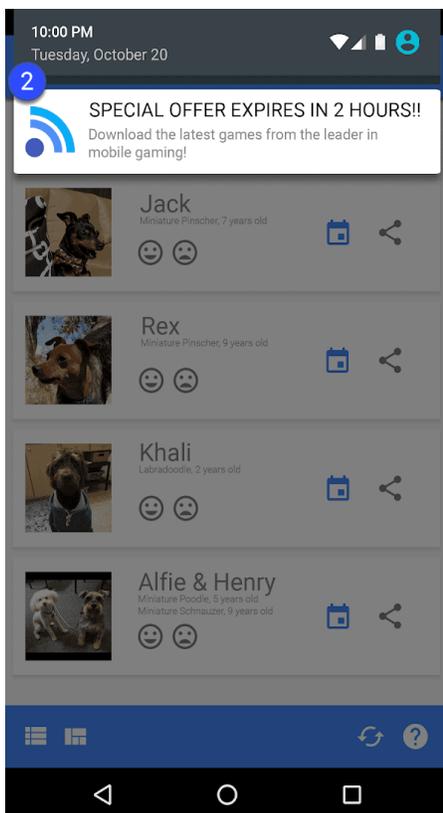
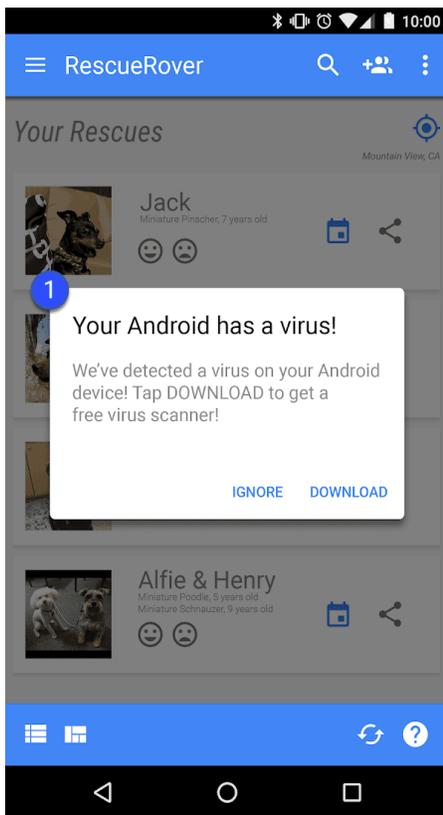
Da Google Play eine sichere und respektvolle Plattform bleiben soll, haben wir Richtlinien entwickelt, in denen schädliche oder unangemessene Inhalte definiert und verboten werden.

- 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 Werbeanzeigen, die verschiedene Systembenachrichtigungen nachahmen.

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.

Störende Werbung

Störende Werbeanzeigen sind Anzeigen, die Nutzern auf unerwartete Weise angezeigt werden. Sie führen zu unbeabsichtigten Klicks und verschlechtern oder beeinträchtigen die Nutzerfreundlichkeit von Gerätefunktionen.

In der App dürfen Nutzer nicht dazu gezwungen werden, auf eine Anzeige zu klicken oder personenbezogene Daten zu Werbezwecken zu senden, damit sie die App vollständig nutzen können. Interstitial-Anzeigen dürfen nur innerhalb der App geschaltet werden, in der sie erscheinen. Wenn in Ihrer App Interstitial-Anzeigen oder sonstige Werbeanzeigen geschaltet werden, die die normale Nutzung beeinträchtigen, müssen sie sich einfach schließen lassen, ohne dass dem Nutzer daraus Nachteile entstehen.

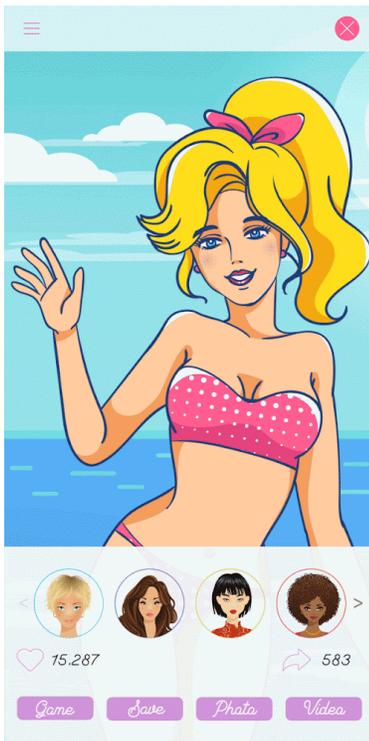
Da Google Play eine sichere und respektvolle Plattform bleiben soll, haben wir Richtlinien entwickelt, in denen schädliche oder unangemessene Inhalte definiert und verboten werden.

- Werbeanzeigen, die den gesamten Bildschirm einnehmen oder die normale Nutzung stören und sich nicht klar sichtbar schließen lassen:

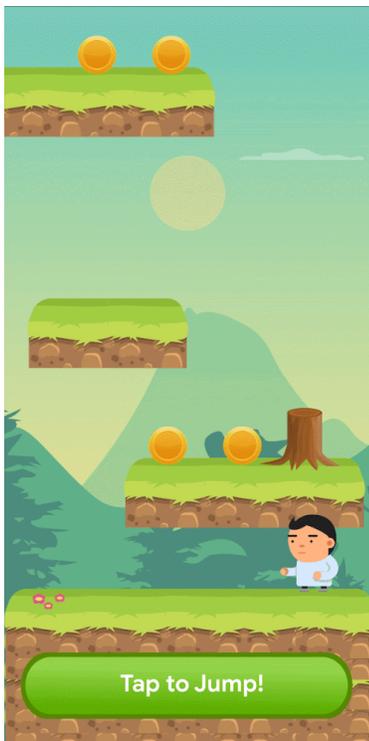


① Diese Werbeanzeige hat keine Schaltfläche zum Schließen.

- Werbeanzeigen, die den Nutzer durch eine falsche "Schließen"-Schaltfläche zum Tippen zwingen oder Werbeanzeigen, die plötzlich in bestimmten Bereichen der App erscheinen, auf die der Nutzer normalerweise für eine andere Funktion tippt.



- Werbeanzeigen, die eine falsche "Schließen"-Schaltfläche verwenden



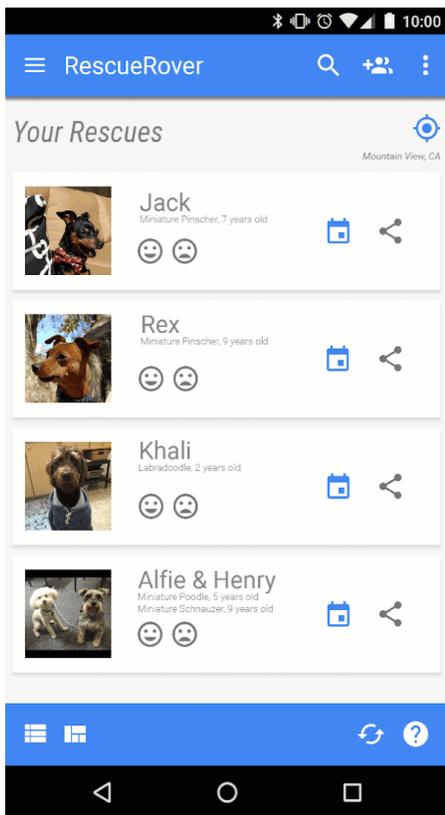
Werbeanzeigen, die plötzlich in einem Bereich erscheinen, in dem der Nutzer normalerweise auf In-App-Funktionen tippt

Beeinträchtigung von Apps, Werbeanzeigen Dritter oder Gerätefunktionen

Mit Ihrer App verbundene Werbeanzeigen dürfen weder andere Apps noch andere Werbeanzeigen oder den Gerätebetrieb beeinträchtigen, darunter System- oder Geräteschaltflächen und -ports. Das gilt unter anderem für Overlays, Companion-Anzeigen und Widget-Anzeigenblöcke. Die Werbeanzeigen dürfen nur innerhalb der jeweiligen App erscheinen.

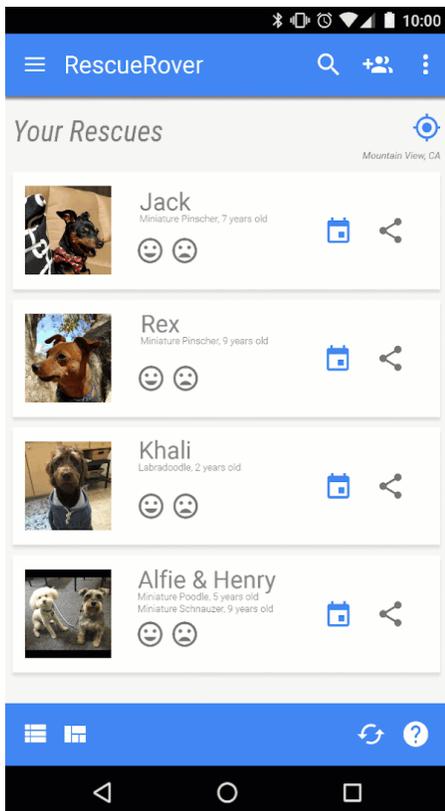
Da Google Play eine sichere und respektvolle Plattform bleiben soll, haben wir Richtlinien entwickelt, in denen schädliche oder unangemessene Inhalte definiert und verboten werden.

- Werbeanzeigen, die außerhalb der jeweiligen App erscheinen:



Beschreibung: Der Nutzer navigiert von dieser App zum Startbildschirm. Plötzlich erscheint eine Werbeanzeige auf dem Startbildschirm.

- Werbeanzeigen, die durch die Schaltfläche für den Startbildschirm oder andere Funktionen ausgelöst werden, die explizit zum Beenden der App konzipiert wurden:

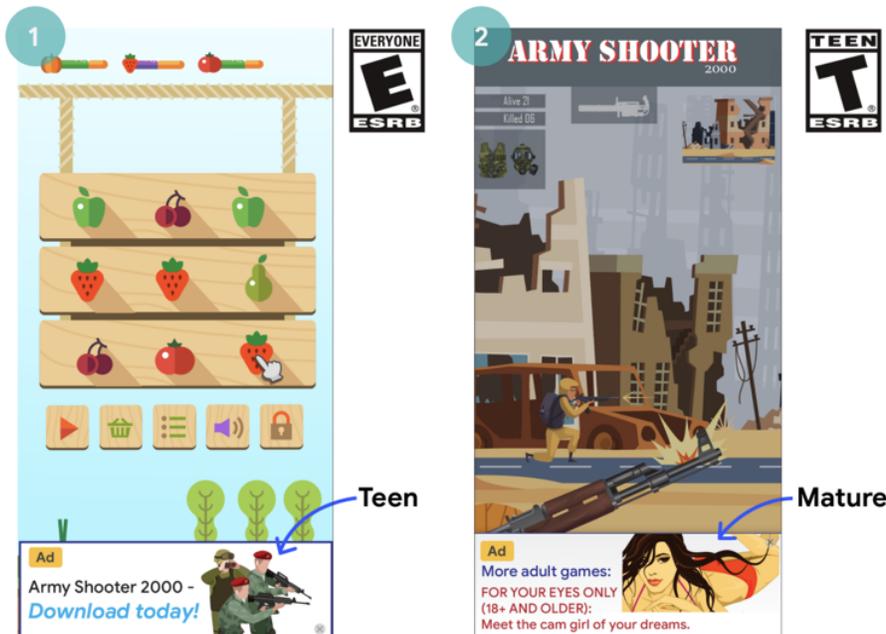


Beschreibung: Der Nutzer versucht, die App zu beenden und zum Startbildschirm zurückzukehren. Stattdessen wird der erwartete Ablauf aber durch eine Werbeanzeige unterbrochen.

Unangemessene Werbung

Der Inhalt von Werbeanzeigen in Ihrer App muss der beabsichtigten Zielgruppe Ihrer App entsprechen, auch wenn der Inhalt der Werbeanzeigen an sich die Richtlinien erfüllt.

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 Diese Werbeanzeige (geeignet für Teenager) ist für die Zielgruppe der App (ab 7 Jahre) unangemessen.
- ② Diese Werbeanzeige (geeignet für Erwachsene) ist für die Zielgruppe der App (ab 12 Jahre) unangemessen.

Verwendung der Android-Werbe-ID

Gültig ab 4. Oktober 2021

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 MAC-Adresse oder IMEI verknüpft werden. Die Werbe-ID darf nur mit ausdrücklicher Zustimmung des Nutzers mit personenidentifizierbaren Informationen verknüpft werden.
 - **Verwendung zur Datenanalyse:** Die Werbe-ID darf nur mit ausdrücklicher Zustimmung des Nutzers mit personenidentifizierbaren Informationen oder gleichbleibenden Geräte-IDs wie MAC-Adresse oder IMEI verknüpft werden. In den [Richtlinien 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 unseren [Richtlinien 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.

Abos

Als Entwickler müssen Sie Nutzer genau darüber aufklären, welche Dienste oder Inhalte das Abo für Ihre App umfasst. Sie dürfen Nutzer niemals absichtlich täuschen. Achten Sie darauf, dass Sie Ihr Angebot bei allen In-App-Werbeaktionen und auf allen Startbildschirmen klar und deutlich kommunizieren.

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

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.
- Preise und Nutzungsbedingungen für Abos, die nicht vollständig lokalisiert sind.
- In-App-Werbeaktionen, bei denen nicht klar ersichtlich ist, dass Nutzer auch ohne Abo auf die Inhalte zugreifen können (sofern möglich).
- Artikelnamen, bei denen die Art des Abos nicht ersichtlich ist. Das ist beispielsweise der Fall, wenn von einer "kostenlosen Testversion" die Rede ist, obwohl dafür regelmäßige Kosten anfallen.

The screenshot shows a subscription offer for 'AnalyzeAPP Premium'. At the top, it says '16 issues found in your data! Subscribe to see how we can help'. Below this are three pricing options: 12 months (\$9.16/mo, Save 35%), 6 months (\$12.50/mo, Save 11%, MOST POPULAR PLAN), and 1 month (\$14.00/mo). A 'Try for \$12.50!' button is highlighted with callout 3. At the bottom, there is a disclaimer in Spanish: '4 Cancele su suscripción en cualquier momento. Por favor, consulte nuestra política de privacidad para más información.'

① Die Schaltfläche "Ablehnen" ist nicht deutlich sichtbar, sodass Nutzer möglicherweise glauben, dass sie nur auf Funktionen zugreifen können, wenn sie ein Abo 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.

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.

Aboverwaltung und -kündigung

Als Entwickler müssen Sie darauf achten, dass in Ihrer/n App(s) leicht verständlich erklärt wird, wie Nutzer ihr Abo verwalten oder kündigen können.

Wenn ein Nutzer ein Abo storniert, das er über eine App bei Google Play erworben hat, besteht gemäß unseren Richtlinien kein Anspruch auf Erstattung für den laufenden Abrechnungszeitraum. Er kann das Abo 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 Abos, Kündigungen und Erstattungen ändern, und dafür zu sorgen, dass die Richtlinien nicht gegen geltendes Recht verstoßen.

Anzeigen in familienfreundlichen Apps

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-SDKs verwenden, die die Google Play-Richtlinien sowie die Zertifizierungsanforderungen für Anzeigen-SDKs einhalten. Ist die App sowohl für Kinder als auch für ältere Nutzer gedacht, müssen Sie Maßnahmen zur Feststellung des Alters ergreifen und gewährleisten, dass Werbung, die Kindern präsentiert wird, ausschließlich von selbstzertifizierten Anzeigen-SDKs stammt. Für Apps im Designed for Families-Programm dürfen ausschließlich selbstzertifizierte Anzeigen-SDKs genutzt werden.

Die Verwendung von Google Play-zertifizierten Anzeigen-SDKs ist nur erforderlich, wenn Sie in Ihrer App Anzeigen-SDKs zur Auslieferung von Werbeanzeigen an Kinder nutzen. 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 Werbeinhalte und Praktiken zur Datenerhebung den [Richtlinien zu Nutzerdaten](#) von Google Play sowie der [Richtlinie für familienfreundliche Inhalte](#) entsprechen:

- Hausinterne Werbung, 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.

Zertifizierungsanforderungen für Anzeigen-SDKs

- 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 Formular unten ausgefüllt wurde, muss sich dessen 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 Publishern das Auswählen von Anzeigenformaten, die den [Richtlinien zu Anzeigen und Monetarisierung in familienfreundlichen Apps von Google Play](#) entsprechen und die Anforderungen des "[Von Lehrern empfohlen](#)"-Programms 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. im unten angegebenen [Formular](#)), damit Google die Erfüllung aller Zertifizierungsanforderungen seitens des Anzeigen-SDK bestätigen kann, und reagieren Sie zeitnah auf mögliche Nachfragen.

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

Vermittlungsanforderungen für Anzeigenschaltungsplattformen bei der Auslieferung von Werbeanzeigen für Kinder:

- Nutzen Sie ausschließlich Google Play-zertifizierte Anzeigen-SDKs 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 die Altersfreigabe für Anzeigeninhalte und gegebenenfalls Inhalte für Kinder anzugeben.

Hier finden Entwickler eine [Liste selbstzertifizierter Anzeigen-SDKs](#) .

Außerdem können Entwickler [dieses Formular](#) an Anzeigen-SDKs weiterleiten, die eine Zertifizierung 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.

Beispiele für häufige Verstöße:

- **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

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

Metadaten

Gültig ab 29. September 2021

Apps mit irreführenden, falsch formatierten, nicht aussagekräftigen, irrelevanten, ausschweifenden 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 Entwicklernamen 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-/Installationsymbole, wenn über die App keine Inhalte heruntergeladen werden können. Der Titel Ihrer App darf maximal 30 Zeichen lang sein.

Zusätzlich zu den hier genannten Anforderungen müssen Sie aufgrund bestimmter Google Play-Richtlinien für Entwickler u. U. 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.

The best way to find a new furry friend!

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

1

See how much our users love us:

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

2

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

50% cooler and 100% faster than FidoFinder

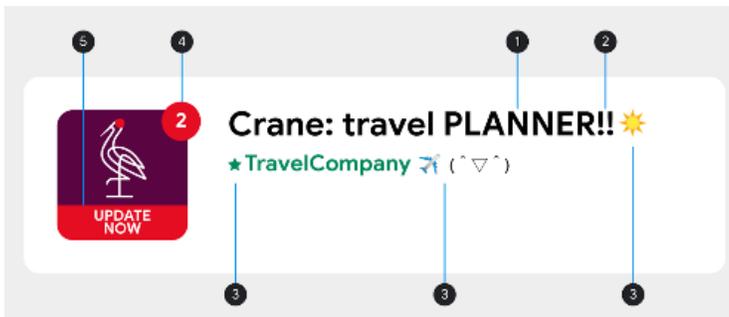
3

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

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



- ① 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

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.
- Darstellung von Gewalt 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 exakt wiedergeben.

- Vermeiden Sie irrelevante oder sich wiederholende Keywords oder Verweise.
- Die Beschreibung Ihrer App sollte kurz, klar und treffend 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 Richtlinienvorstoß 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.

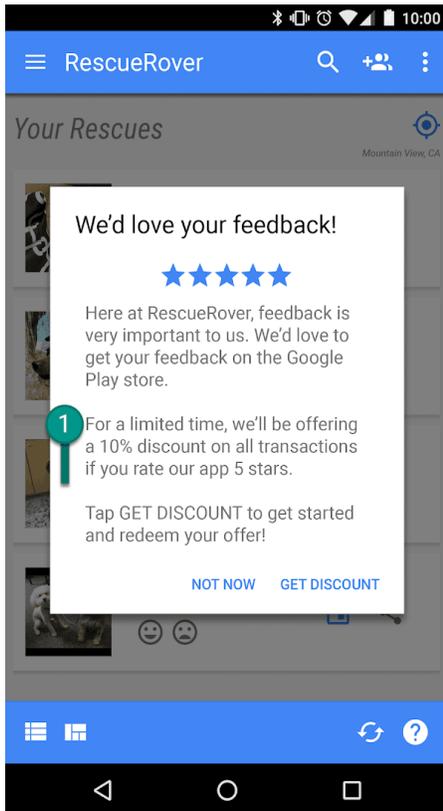
Bewertungen, Rezensionen und Installationen von Nutzern

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 Anreize motivierte Installationen, Rezensionen und Bewertungen. Das ist zum Beispiel der Fall, wenn Texte oder Bilder in Ihrem App-Titel, im Symbol oder im Entwicklernamen den Preis oder andere Werbeinformationen enthalten.

Entwickler dürfen im App-Titel, Symbol oder Entwicklernamen keine Texte oder Bilder hinzufügen, die auf die Leistung oder das Ranking im Play Store hinweisen oder eine Verbindung mit vorhandenen Google Play-Programmen nahelegen.

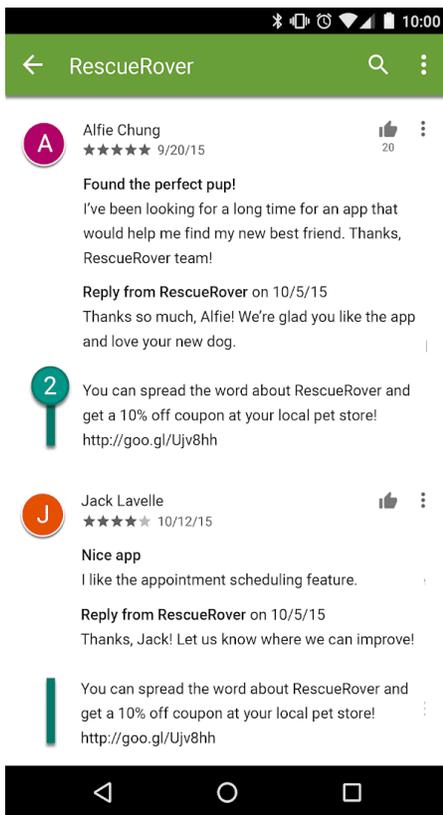
Da Google Play eine sichere und respektvolle Plattform bleiben soll, haben wir Richtlinien entwickelt, in denen schädliche oder unangemessene Inhalte definiert und verboten werden.

- Nutzer durch Incentives zur Bewertung Ihrer App bewegen:



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

- Wiederholte Abgabe von Bewertungen, um die Platzierung der App bei Google Play zu beeinflussen
- Abgabe von Rezensionen oder Aufforderung zur Abgabe von Rezensionen mit unangemessenen Inhalten wie Partnerinhalte, Gutscheine, Spielcodes, E-Mail-Adressen oder Links zu Websites oder anderen Apps:



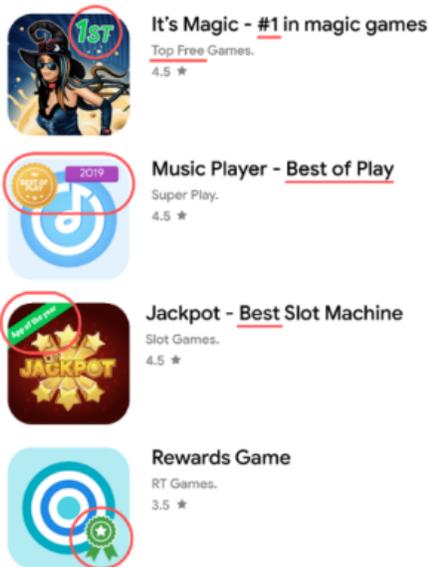
② Diese Rezension fordert Nutzer durch ein Gutscheinangebot auf, Werbung für die RescueRover App zu machen.

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 Rezensionen:

- 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.

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

- 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.



O Basket - \$50 Cashback
Digital Brand.
4.5 ★



Gmart - On Sale For Limited Time
Shop Limited.
4.3 ★



Fish Pin- Free For Limited Time Only
Entertainment Play.
4.5 ★



Golden Slots Fever: Free 100
Gamepub Play.
4.2 ★

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



Build Roads - New Game
KDG Games.
3.5 ★



Robot Game - Editor's choice
Entertainment Games.
4.5 ★

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 App, die in der Play Console als Nachrichten-App deklariert ist („Nachrichten-Apps“), muss alle folgenden Anforderungen erfüllen.

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

Nachrichten-Apps **MÜSSEN**:

- Informationen zu Eigentumsrechten des Nachrichtenverlags und dessen Beitragenden enthalten, einschließlich, aber nicht beschränkt auf eine Angabe der offiziellen Website für die in der App veröffentlichten Nachrichten, außerdem gültige und überprüfbare Kontaktdaten sowie den ursprünglichen Publisher jedes Artikels
- eine spezielle Website oder In-App-Seite bieten, die eindeutig als Kontaktdaten enthaltend gekennzeichnet ist, leicht zu finden ist (z. B. über einen Link unten auf der Startseite oder in der Navigationsleiste der Website) und gültige Kontaktdaten zu dem Nachrichtenverlag enthält, darunter mindestens eine Kontakt-E-Mail-Adresse und -Telefonnummer.

Beachten Sie, dass Links zu Konten in sozialen Medien keine ausreichende Form von Kontaktdaten darstellen. Ferner sollten Apps, die hauptsächlich von Nutzern erstellte Inhalte enthalten (z. B. Apps für soziale Medien), nicht als Nachrichten-Apps deklariert werden.

Nachrichten-Apps **DÜRFEN NICHT**:

- erhebliche Rechtschreib- oder Grammatikfehler enthalten
- nur statischen Content enthalten, z. B. Inhalte, die mehrere Monate alt sind
- Affiliate-Marketing oder Werbeeinnahmen 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 Richtlinienanforderungen 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

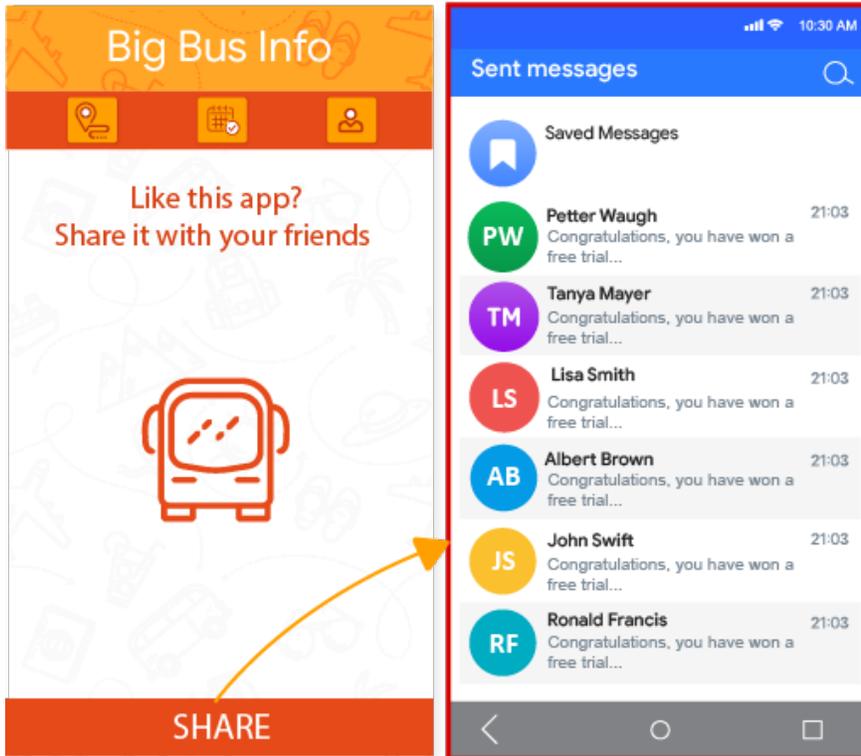
Wir gestatten keine Apps, die Nutzer oder Google Play spammen, etwa Apps, die Nutzern unerwünschte Nachrichten senden, sowie sich wiederholende und minderwertige Apps.

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:

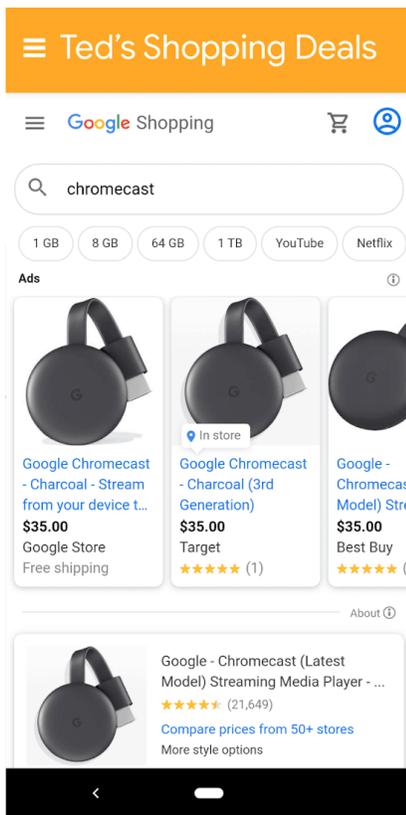


Spam zum Generieren von Seitenzugriffen und Affiliate-Spam

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 Gutscheine 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:



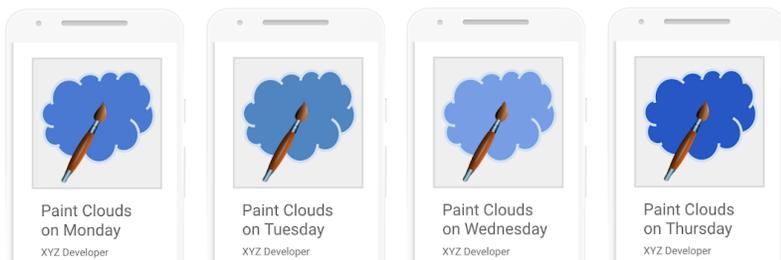
① Die App heißt „Ted’s Shopping Deals“, zeigt aber lediglich eine Webansicht von Google Shopping.

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.



Werbe-Apps

Apps, deren wesentlicher Zweck im Ausliefern von Anzeigen besteht, 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.

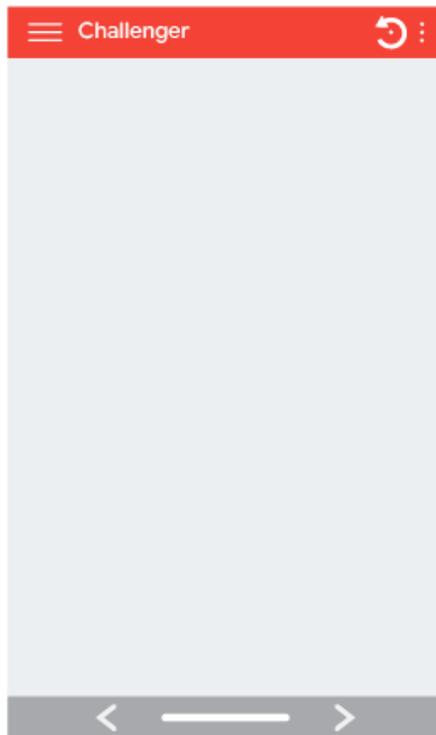
- Apps, in denen Interstitial-Anzeigen nach jeder Nutzeraktion eingeblendet werden. Zu Nutzeraktionen gehören u. a. Klicks und Wischbewegungen.

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



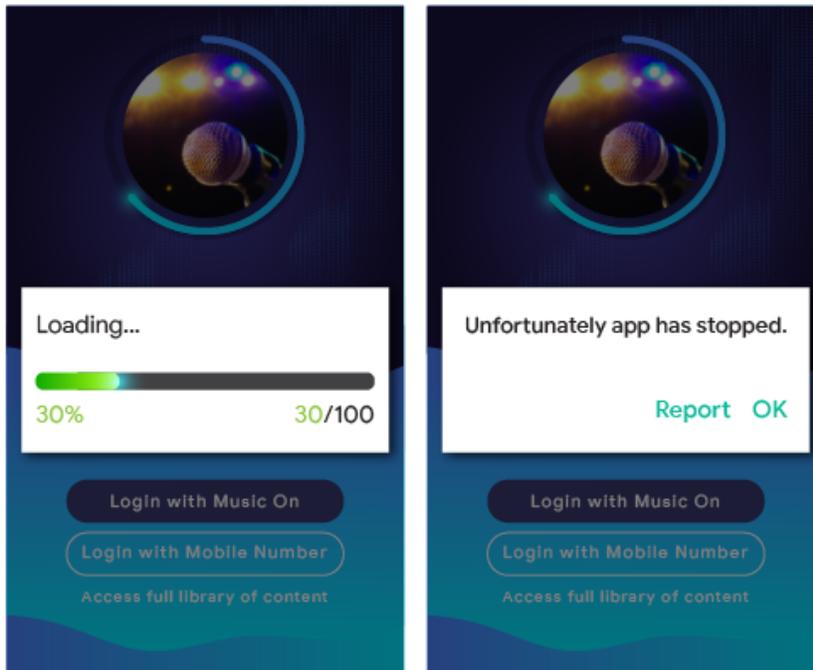
Fehlerhafte Funktionen

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

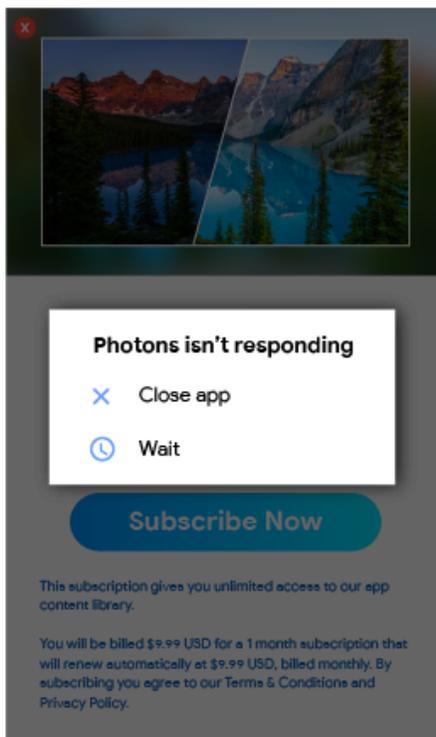
Da Google Play eine sichere und respektvolle Plattform bleiben soll, haben wir Richtlinien entwickelt, in denen schädliche oder unangemessene Inhalte definiert und verboten werden.

- 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](#).

Gerätstatus 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.

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.](#)

Apps für Kinder und Familien

Technik 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.

Apps, die speziell für Kinder entwickelt wurden, müssen für das Designed for Families-Programm angemeldet werden. Auch wenn Ihre App sowohl für Kinder als auch für ältere Zielgruppen entwickelt wurde, können Sie am Designed for Families-Programm teilnehmen. Alle Apps, die am Designed for Families-Programm teilnehmen, können für das ["Von Lehrern empfohlen"-Programm](#) bewertet werden. Wir können jedoch nicht garantieren, dass Ihre App in das "Von Lehrern empfohlen"-Programm aufgenommen wird. Sollten Sie sich gegen die Teilnahme am Designed for Families-Programm entscheiden, sind Sie dennoch dazu verpflichtet, sich an die Google Play-Richtlinien für familienfreundliche Inhalte weiter unten sowie alle sonstigen [Google Play-Programmrichtlinien für Entwickler](#) und die [Vertriebsvereinbarung für Entwickler](#) zu halten.

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-Eintragseite 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.
- 2. App-Funktionalität:** Ihre App darf nicht nur eine Webansicht einer Website darstellen oder dem Hauptzweck dienen, Nutzer auf Affiliate-Websites weiterzuleiten, unabhängig davon, wer der Inhaber der Website ist.
 - Wir suchen ständig nach Möglichkeiten, Entwicklern von Apps für Kinder neue Verbesserungen zu bieten. Wenn Sie Teil unseres „Trusted Web App“-Pilotprojekts für Lern-Apps werden möchten, [informieren Sie uns hier](#) über Ihr Interesse.
- 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 die interaktiven Elemente der App im Fragebogen zur Einstufung des Inhalts genau darstellen. Beispiele:
 - Nutzer Ihrer App können mit anderen Nutzern interagieren oder Informationen austauschen,
 - Nutzer Ihrer App können bereitgestellte Daten an Drittanbieter weitergeben und
 - Ihre App teilt den Standort des Nutzers mit anderen Nutzern.
- 4. Anzeigen:** Wenn Kindern oder Nutzern unbekanntes Alter in Ihrer App Werbung präsentiert wird, ist Folgendes zu beachten:
 - Werbung darf diesen Nutzern nur über [Google Play-zertifizierte Anzeigen-SDKs](#) präsentiert werden
 - 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
 - Werbeanzeigen, die diesen Nutzern angezeigt werden, müssen für Kinder geeignet sein
 - Werbung, die diesen Nutzern angezeigt wird, muss den Formatanforderungen für Werbeanzeigen von Designed for Families entsprechen
 - alle geltenden rechtlichen Vorschriften und Branchenstandards im Hinblick auf Werbeanzeigen für Kinder müssen erfüllt werden.
- 5. 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:
 - Sie dürfen keine Android-Werbe-ID (Android Advertising Identifier, AAID), SIM-Seriennummer, Build-Seriennummer, BSSID, MAC-Adresse, SSID, IMEI und/oder IMSI von Kindern oder Nutzern unbekanntes Alters übertragen.
 - Telefonnummern des Geräts dürfen nicht über TelephonyManager der Android API angefordert werden.
 - Apps, die ausschließlich für Kinder bestimmt sind, dürfen nicht den Standort des Nutzers anfragen, 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.
- 6. APIs und SDKs:** Sie müssen gewährleisten, dass APIs und SDKs ordnungsgemäß in Ihrer App implementiert sind.
 - Apps, die ausschließlich für Kinder bestimmt sind, dürfen keine APIs oder SDKs enthalten, die nicht für die Verwendung in auf Kinder ausgerichteten Diensten zugelassen sind. Dazu zählen der Google Log-in und alle sonstigen Google-API-Dienste mit Zugriff auf Daten, die mit einem Google-Konto verknüpft sind, außerdem die Google Play-Spieldienste sowie jegliche sonstigen API-Dienste, bei denen OAuth-Technologie zur Authentifizierung und Autorisierung eingesetzt wird.
 - 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 zur Anmeldung oder zum Zugriff auf App-Inhalte durch Nutzer keine APIs oder SDKs zum Einsatz kommen, die nicht für die Verwendung in Inhalten für Kinder zugelassen sind.
- 7. 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 elterlichen Aufsicht 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).

8. Einhaltung gesetzlicher Bestimmungen: Sie müssen gewährleisten, 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 Darstellung von Gewalt, pornografische Inhalte oder Glücksspielbezogene Inhalte. [Weitere Informationen zu den Google Play-Richtlinien für Werbung, In-App-Käufe und kommerzielle Inhalte für Kinder in den Richtlinien für Anzeigen und Monetarisierung in familienfreundlichen Inhalten](#)

Das Designed for Families-Programm

Apps, die speziell für Kinder entwickelt wurden, müssen für das Designed for Families-Programm angemeldet werden. Auch wenn Ihre App für alle Nutzer, einschließlich Kindern und Familien, entwickelt wurde, können Sie sich zur Teilnahme an dem Programm anmelden.

Damit Sie für das Programm zugelassen werden, muss Ihre App alle Anforderungen der Richtlinie für familienfreundliche Inhalte sowie die Teilnahmevoraussetzungen für Designed for Families erfüllen. Außerdem muss sie den [Google Play-Programmrichtlinien für Entwickler](#) und der [Vertriebsvereinbarung für Entwickler](#) entsprechen.

Weitere Informationen dazu, wie Sie Ihre App für das Programm anmelden können, [finden Sie hier](#) .

Teilnahmevoraussetzungen

Alle Apps im Designed for Families-Programm dürfen nur App- und Werbeanzeigeninhalte enthalten, die für Kinder relevant und geeignet sind, und dürfen nur [Google Play-zertifizierte Anzeigen-SDKs](#) verwenden. Die Apps müssen die ESRB-Altersfreigabe „Everyone“ (Jedes Alter) bzw. „Everyone 10+“ (Nutzer ab 10 Jahren) oder die entsprechende regionale Einstufung haben. In das Programm aufgenommene Apps müssen allen Programmanforderungen entsprechen. Google Play kann jede App ablehnen, entfernen oder sperren, die als unangemessen für das Designed for Families-Programm eingestuft wurde.

Hier sind einige Beispiele für Apps, die nicht für das Programm infrage kommen:

- Apps mit der ESRB-Einstufung "Everyone" (Jedes Alter), die Werbeanzeigen zu Glücksspielen beinhalten
- Apps für Eltern oder Betreuer – z. B. eine App zur Erfassung von Stillzeiten oder ein Ratgeber zur Kindesentwicklung
- Apps, die als Leitfaden für Eltern oder zur Geräteverwaltung dienen und nur für die Nutzung durch Eltern oder Betreuer bestimmt sind

Kategorien

Wird Ihre App in das Designed for Families-Programm aufgenommen, können Sie eine zweite programmspezifische Kategorie zur Beschreibung der App auswählen. Folgende Kategorien stehen für Apps im Designed for Families-Programm zur Auswahl:

Action & Abenteuer: Action-orientierte Apps und Spiele – von Rennsportspielen über Märchenabenteuer bis hin zu anderen Apps und Spielen, die Spannung erzeugen sollen

Denkspiele: Spiele, bei denen die Nutzer viel nachdenken müssen – z. B. Rätsel, Memory-Spiele, Quiz und andere Spiele, die das Gedächtnis bzw. den Intellekt auf die Probe stellen oder logisches Denken erfordern

Kreativität: Apps und Spiele, die die Kreativität fördern – z. B. Apps zum Zeichnen, Malen oder Programmieren sowie andere Apps und Spiele, mit denen man etwas gestalten und entwickeln kann

Bildung: Apps und Spiele, die mithilfe von Bildungsexperten (z. B. Pädagogen, Entwicklern von Lerninhalten oder Forschern) entwickelt wurden, um Lernprozesse zu fördern – dazu zählt wissenschaftliches, sozio-emotionales, körperliches und kreatives Lernen sowie die Aneignung von grundlegenden Alltagsfähigkeiten, kritischem Denken und Problemlösefähigkeiten

Musik und Videos: Apps und Spiele, bei denen es um Musik oder Videos geht – von Apps zur Simulation von Instrumenten bis hin zu solchen, die Video- und Musikinhalte bieten

Rollenspiele: Apps und Spiele, bei denen der Nutzer eine bestimmte Rolle einnehmen kann – z. B. die eines Kochs, einer Pflegekraft, einer Prinzessin bzw. eines Prinzen, eines Feuerwehrmanns, eines Polizisten oder einer fiktiven Figur

Anzeigen und Monetarisierung

Die Richtlinien weiter unten gelten für jede Art von Werbung in Ihrer App, einschließlich Werbung für Ihre eigenen Apps als auch für Drittanbieter-Apps, für In-App-Kaufangebote sowie für alle sonstigen kommerziellen Inhalte – z. B. bezahltes Produkt-Placement –, die Nutzern von Apps angezeigt werden, welche den Richtlinien für familienfreundliche Inhalte und/oder von Designed for Families unterliegen. Alle Werbeanzeigen, In-App-Kaufangebote und kommerziellen Inhalte 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.

Formatanforderungen für Werbung

Werbeanzeigen und In-App-Kaufangebote dürfen grundsätzlich keine irreführenden Inhalte haben. Außerdem dürfen sie nicht so gestaltet sein, dass Kinder zu unbeabsichtigten Klicks verleitet werden. Folgendes ist untersagt:

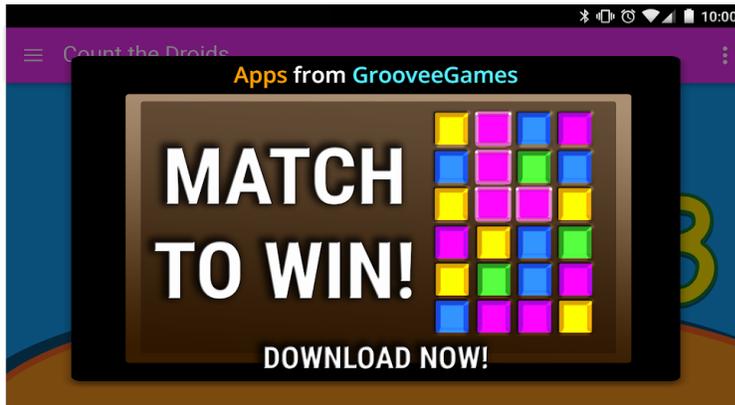
- Störende Werbung, einschließlich Anzeigen, die den gesamten Bildschirm einnehmen oder die normale Nutzung beeinträchtigen und bei denen die Schaltfläche zum Schließen nicht deutlich sichtbar ist, z. B. [Blockierungen durch Anzeigen](#)
- Anzeigen, die die normale Verwendung der App oder den Spielverlauf beeinträchtigen und sich nicht nach 5 Sekunden schließen lassen. Anzeigen, die die normale App-Nutzung oder das normale Spiel nicht beeinträchtigen, können länger als 5 Sekunden eingeblendet werden, z. B. Videoinhalte mit integrierten Anzeigen.
- Interstitial-Anzeigen oder In-App-Kaufangebote, 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.
- Werbeanzeigen oder In-App-Kaufangebote, 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.

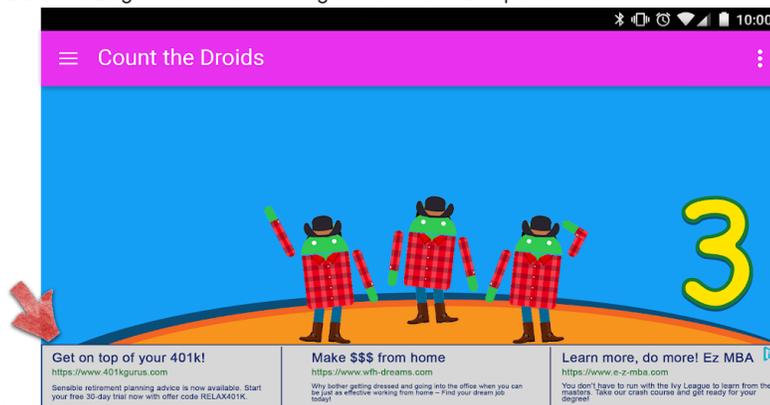
- Werbeanzeigen, die sich vom Finger des Nutzers wegbewegen, wenn dieser versucht, sie zu schließen
- Werbeanzeigen, die wie im Beispiel unten dem Nutzer keine Möglichkeit bieten, die Werbung nach fünf (5) Sekunden zu schließen:



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



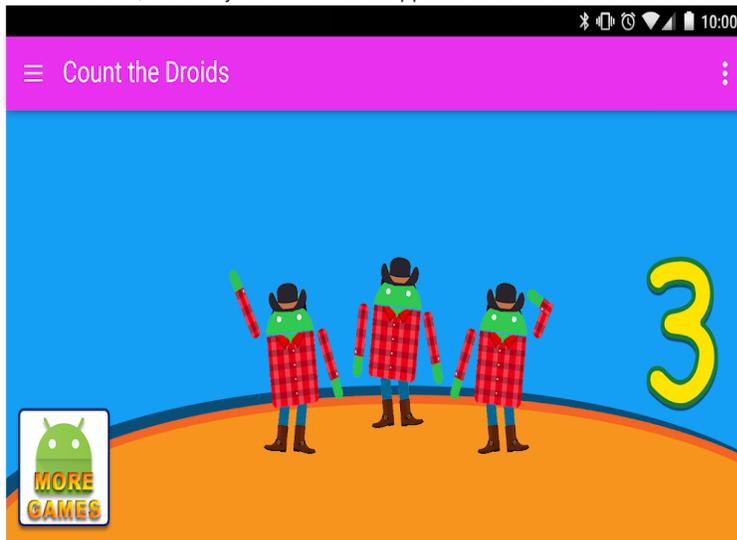
- Banneranzeigen mit mehreren Angeboten wie im Beispiel unten:



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



- Schaltflächen oder Werbeanzeigen 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 einblenden und Ihre Zielgruppe nur Kinder umfasst, müssen Sie [Google Play-zertifizierte Anzeigen-SDKs](#) 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 Google Play-zertifizierten Anzeigen-SDKs stammt. Für Apps im Designed for Families-Programm dürfen ausschließlich selbstzertifizierte Anzeigen-SDKs genutzt werden.

Weitere Einzelheiten zu diesen Anforderungen sowie eine Liste zugelassener SDKs finden Sie auf der Seite [Anzeigen in familienfreundlichen Apps](#).

Wenn Sie AdMob verwenden, finden Sie weitere Details zu den entsprechenden Produkten in der [AdMob-Hilfe](#).

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.

In-App-Käufe

Bei Google Play werden alle Nutzer vor einem In-App-Kauf in Apps des Designed for Families-Programms noch einmal authentifiziert. Diese Maßnahme soll dazu beitragen, dass nicht ein Kind, sondern die finanziell verantwortliche Person den Kauf abschließt.

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

Wenn Ihre App gegen eine unserer Richtlinien verstößt, ergreifen wir die unten beschriebenen Maßnahmen. 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 irrtümlich Maßnahmen ergriffen haben.

Beachten Sie, dass in Mitteilungen bezüglich Entfernungen oder administrativen Mitteilungen möglicherweise nicht alle in 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 restliche App den Richtlinien entspricht. Wenn Sie Richtlinienverstöße nicht in 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 schaden, haben die Kündigung der beteiligten Google Play-Entwicklerkonten zur Folge.

Durchsetzungsmaßnahmen

Unterschiedliche Maßnahmen zur Durchsetzung können unterschiedliche Auswirkungen auf Ihre App haben. 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. Diese Informationen werden auch in [diesem Video](#) erläutert.

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 den Store-Eintrag, die Installationen durch Nutzer, Statistiken und Bewertungen der App nicht 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 den Store-Eintrag, die Installationen durch Nutzer, Statistiken und Bewertungen der App nicht 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 Sie Ihre App in den Status "Eingeschränkte Sichtbarkeit" versetzt wurde, hat dies keine Auswirkungen auf den Status Ihres Google Play-Entwicklerkontos.
- Wenn Sie Ihre App in den Status "Eingeschränkte Sichtbarkeit" versetzt wurde, hat dies keinen Einfluss darauf, ob Nutzer den vorhandenen Store-Eintrag, die Installationen durch Nutzer, Statistiken und Bewertungen der App sehen können.

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 die Kündigung Ihres Play Console-Kontos zur Folge haben.
- Da die Apps des gekündigten Kontos entfernt werden, können Nutzer den Store-Eintrag der App, die Installationen durch Nutzer, Statistiken und Bewertungen nicht sehen.

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

Ihre App wird wieder im Play Store veröffentlicht, falls ein Fehler vorlag und wir feststellen, dass die 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, um Einspruch zu erheben.

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, die die Überprüfung Ihrer App verzögern oder zu einer Ablehnung führen können, bitten wir Sie, die nachfolgenden Punkte unbedingt zu beachten, wenn Sie Informationen über die Play Console senden.

Achten Sie darauf, dass folgende Voraussetzungen erfüllt sind, bevor Sie Ihre App einreichen:

- Alle App-Informationen und -Metadaten wurden korrekt angegeben.
- Ihre Kontaktdaten sind aktuell.
- Sie haben die Datenschutzerklärung Ihrer App hochgeladen und die mit dem Abschnitt zur **Datensicherheit** verbundenen Anforderungen erfüllt.
- Sie haben ein aktives Demokonto, Anmeldeinformationen und alle weiteren Ressourcen angegeben, die zur Überprüfung Ihrer App benötigt werden, z. B. Anmeldedaten oder ein 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 [Programmrichtlinien für Entwickler](#) von Google Play 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