App-Prüfungsrichtlinien

Apps verändern die Welt, bereichern das Leben der Menschen und ermöglichen Entwickler:innen wie Ihnen, in bisher unbekanntem Maße Innovationen voranzutreiben. Infolgedessen hat sich der App Store zu einem spannenden und aktiven Ökosystem für Millionen von Entwickler:innen und mehr als eine Milliarde Nutzer:innen entwickelt. Egal, ob Sie gerade Ihre erste App entwickeln oder Teil eines großen Teams erfahrener Programmierer:innen sind: Wir freuen uns, dass Sie Apps für den unsere Plattformen erstellen, und möchten Ihnen helfen, unsere Richtlinien zu verstehen, damit Sie sicher sein können, dass Ihre App den Überprüfungsprozess schnell erfolgreich durchlaufen wird.

April 2024

Einführung **4**

Vor dem Einreichen **5**

1. Sicherheit **6**

1.1 Anstößige Inhalte 7

1.2 Nutzergenerierte Inhalte 7

1.2.1 Creator-Inhalte 8

1.3 Kategorie „Kinder“ 8

1.4 Körperliche Schäden 9

1.5 Entwicklerinformationen 9

1.6 Datensicherheit 10

1.7 Meldung krimineller Aktivitäten 10

2. Leistung **10**

2.1 Vollständigkeit der App 10

2.2 Betatests 10

2.3 Genaue Metadaten 11

2.4 Hardwarekompatibilität 13

2.5 Softwarevoraussetzungen 14

3. Geschäfte **17**

3.1 Zahlungen 17

3.1.1 In-App-Käufe 17

3.1.1(a) Link zu anderen Kaufmethoden 18

3.1.2 Abonnements 19

3.1.2 (a) Zulässige Verwendungen 19

3.1.2(b) Upgrades und Downgrades: 20

3.1.2(c) Abonnementinformationen 20

3.1.3 Weitere Kaufmethoden 21

3.1.3(a) „Reader“-Apps 21

3.1.3(b) Plattformübergreifende Dienste 21

3.1.3(c) Unternehmensdienste 21

3.1.3(d) Persönliche Dienste 21

3.1.3(e) Waren und Dienste außerhalb der App 21

3.1.3(f) Kostenlose eigenständige Apps 22

3.1.3(g) Werbemanagement-Apps 22

3.1.4 Hardwarespezifische Inhalte 22

3.1.5 Kryptowährungen 22

3.2 Andere Probleme mit dem Geschäftsmodell 23

3.2.1 Zulässig 23

3.2.2 Nicht zulässig 24

4. Design **25**
4.1 Nachahmer 25
4.2 Mindestfunktionalität 25
4.2.7 Remote Desktop Clients 26
4.3 Spam 26
4.4 Erweiterungen 27
4.5 Apple Websites und Dienste 28
4.6 Alternative App-Symbole 29
4.7 Mini-Apps, Mini-Spiele, Streamingspiele, Chatbots, Plug-ins und Spiel-Emulatoren 29
4.8 Anmeldedienste 30
4.9 Apple Pay 31
4.10 Monetarisierung integrierter Funktionen 31
5. Rechtliche Hinweise **31**
5.1 Datenschutz 31
5.1.1 Datenerfassung und -speicherung 32
5.1.2 Datennutzung und -freigabe 33
5.1.3 Gesundheit und Gesundheitsforschung 34
5.1.4 Kinder 35
5.1.5 Ortungsdienste 36
5.2 Geistiges Eigentum 36
5.3 Spiele, Glücksspiel und Lotterien 37
5.4 VPN-Apps 38
5.5 Mobile Geräteverwaltung 38
5.6 Verhaltenskodex für Entwickler:innen 38
5.6.1 Rezensionen im App Store 39
5.6.2 Identität von Entwickler:innen 39
5.6.3 Betrug 39
5.6.4 App-Qualität 39
Nach dem Einreichen **40**

Einführung

Das Leitprinzip des App Store ist einfach: Wir möchten Nutzer:innen eine sichere Plattform bieten, über die sie Apps beziehen können – und Entwickler:innen eine großartige Gelegenheit, erfolgreich zu sein. Dazu bieten wir einen stark kuratierten App Store an, in dem jede App von Experten geprüft wird und ein Redaktionsteam den Nutzer:innen hilft, jeden Tag neue Apps zu entdecken. Außerdem scannen wir jede App auf Malware und andere Software, die sich auf die Sicherheit, Privatsphäre und den Datenschutz der Nutzer:innen auswirken können. Diese Maßnahmen haben dafür gesorgt, dass die Plattformen von Apple weltweit die sichersten für Endverbraucher:innen sind.

In der Europäischen Union können Entwickler:innen außerdem beglaubigte iOS Apps über alternative App-Marktplätze verteilen. Erfahren Sie mehr über alternative App-Marktplätze und die Beglaubigung von iOS Apps. Sie können sehen, welche Richtlinien für die Beglaubigung von iOS Apps gelten, indem Sie im Menü links auf „Nur Richtlinien für die Beglaubigungsüberprüfung anzeigen“ klicken.

Für alles andere gibt es das offene Internet. Wenn sich das Modell und die Richtlinien des App Store oder alternative App-Marktplätze und die Beglaubigung von iOS Apps für Ihre App oder Geschäftsidee nicht gut eignen, bieten wir zudem Safari für ein großartiges Weberlebnis an.

Auf den folgenden Seiten finden Sie unsere neuesten Richtlinien in fünf klaren Abschnitten: „Sicherheit“, „Leistung“, „Unternehmen“, „Design“ und „Rechtliche Hinweise“. Der App Store wird ständig überarbeitet und verbessert, um mit den Anforderungen unserer Kund:innen und Produkte Schritt zu halten. Und auch Ihre Apps sollten ständig überarbeitet und verbessert werden, um im App Store zu bleiben.

Einige weitere Punkte, die Sie beim Verteilen Ihrer App auf unseren Plattformen beachten sollten:

• Es gibt viele Kinder, die im App Store viele Apps laden. Die Kindersicherung funktioniert großartig, um Kinder zu schützen, aber auch Sie müssen Ihren Teil dazu beitragen. Wir behalten die Sicherheit der Kinder im Auge.

• Der App Store ist eine großartige Möglichkeit, um Hunderte Millionen von Menschen auf der ganzen Welt zu erreichen. Wenn Sie einfach nur eine App Ihrer Familie und Freunden zeigen möchten, ist der App Store nicht der beste Weg. Erwägen Sie stattdessen die Verwendung von Xcode, um Ihre App kostenlos auf einem Gerät zu installieren, oder verwenden Sie die Ad-hoc-Verteilung, die Mitgliedern des Apple Developer Program zur Verfügung steht. Wenn Sie gerade erst anfangen, erfahren Sie hier mehr über das Apple Developer Program.

• Wir setzen uns dafür ein, dass alle Standpunkte im App Store vertreten sind, solange die Apps Nutzer:innen mit abweichenden Meinungen respektieren und die App-Qualität den Anforderungen entspricht. Apps für Inhalte oder Verhaltensweisen, die unserer Meinung nach über das Ziel hinausschießen, lehnen wir ab. Aber wie erkennt man, ob das der Fall ist? Ein Richter des Supreme Court in den USA drückte es einmal so aus: „Ich erkenne es, wenn ich es sehe“. Wir glauben, dass Sie selbst erkennen werden, wenn Sie über das Ziel hinausschießen.

• Wenn Sie versuchen, das System zu hintergehen (z. B. den Überprüfungsprozess auszutricksen, Nutzerdaten zu stehlen, die Arbeit anderer Entwickler:innen zu kopieren oder Rezensionen oder die App Store-Entdeckung zu manipulieren), werden Ihre Apps aus dem App Store entfernt. Außerdem werden Sie aus dem Apple Developer Program ausgeschlossen.

• Sie sind dafür verantwortlich, dass Ihre App in vollem Umfang diesen Richtlinien entspricht, einschließlich Anzeigennetzwerken, Analysediensten und SDKs von Drittanbietern. Überprüfen und wählen sie diese daher sorgfältig aus.

• Einige Funktionen und Technologien, die Entwickler:innen im Allgemeinen nicht zur Verfügung stehen, können für eingeschränkte Anwendungsfälle als Berechtigung angeboten werden. Wir bieten beispielsweise Berechtigungen für CarPlay Audio, HyperVisor und Privileged File Operations an. Weitere Informationen zu Berechtigungen finden Sie in unserer Dokumentation auf developer.apple.com.

Wir hoffen, dass diese Richtlinien Ihnen dabei helfen, den Überprüfungsprozess problemlos zu durchlaufen, und dass Genehmigungen und Ablehnungen einheitlich bleiben. Dieses Dokument wird ständig überarbeitet. Neue Apps, die neue Fragen aufwerfen, können jederzeit zu neuen Regeln führen. Möglicherweise ist es sogar Ihre App, die eine solche Überarbeitung erforderlich macht. Auch das wissen wir zu schätzen und wir würdigen Ihre Arbeit. Wir tun wirklich unser Bestes, um die beste Plattform der Welt anzubieten, damit Sie Ihre Talente zum Ausdruck bringen und auch Ihren Lebensunterhalt verdienen können.

Vor dem Einreichen

Damit die Genehmigung Ihrer App so reibungslos wie möglich abläuft, sollten Sie die unten aufgeführten häufigen Fehler prüfen, die möglicherweise den Überprüfungsprozess verlangsamen oder zu einer Ablehnung führen. Dadurch werden die Richtlinien oder die Garantiegenehmigung nicht ersetzt, aber es ist ein guter Anfang, alle Punkte auf der Liste zu überprüfen. Wenn Ihre App nicht mehr wie vorgesehen funktioniert oder Sie sie nicht mehr aktiv Support dafür bereitstellen, wird sie aus dem App Store entfernt. Erfahren Sie mehr über Verbesserungen des App Store.

Stellen Sie Folgendes sicher:

- Testen Sie Ihre App auf Abstürze und Fehler.
- Vergewissern Sie sich, dass alle App-Informationen und Metadaten vollständig und korrekt sind.
- Halten Sie Ihre Kontaktinformationen aktuell, falls App Review Sie erreichen muss.
- Ermöglichen Sie App Review den vollständigen Zugriff auf Ihre App. Wenn Ihre App accountbasierte Features umfasst, stellen Sie entweder einen aktiven Demoaccount oder einen voll ausgestatteten Demomodus sowie weitere Hardware oder Ressourcen bereit, die für die Überprüfung Ihrer App erforderlich sind (z. B. Anmeldedaten oder einen Beispiel-QR-Code).
- Aktivieren Sie die Backend-Dienste, sodass das App Review Team auf sie zugreifen kann.

- Machen Sie in den Notizen für App Review detaillierte Angaben zu nicht offensichtlichen Features und In-App-Käufen, gegebenenfalls einschließlich begleitender Dokumentation.
- Prüfen Sie, ob Ihre App weiteren Richtlinien wie denen in den folgenden Dokumenten entspricht:

Development Guidelines (Entwicklungsrichtlinien)

UIKit
AppKit
WatchKit
App-Erweiterungen
iOS Data Storage Guidelines (iOS Datenspeicherrichtlinien)
Apple File System (Apple Dateisystem)
App Store Connect Help (App Store Connect Hilfe)
Developer Account Help (Entwickleraccount-Hilfe)

Design Guidelines (Design-Richtlinien)

Human Interface Guidelines (Richtlinien für Nutzerschnittstellen)

Brand and Marketing Guidelines (Marken- und Marketingrichtlinien)

Marketing Resources and Identity Guidelines (Marketingressourcen und Identitätsrichtlinien)
Apple Pay Marketing Guidelines (Marketingrichtlinien für Apple Pay)
Add to Apple Wallet Guidelines (Richtlinien für das Hinzufügen zu Apple Wallet)
Guidelines for Using Apple Trademarks and Copyrights (Richtlinien zur Verwendung von marken- oder urheberrechtlich geschützten Apple Materialien)

Richtlinien, die 🕶 umfassen, gelten für die Beglaubigung von iOS Apps in der EU.

---

1. Sicherheit

Wenn Nutzer:innen eine App aus dem App Store installieren, möchten sie darauf vertrauen können, dass sie sicher ist – dass die App also keine störenden oder beleidigenden Inhalte enthält, ihr Gerät nicht beschädigt und durch die Verwendung voraussichtlich keine körperlichen Schäden verursachen wird. Nachfolgend finden Sie eine Auflistung der wichtigsten Ablehnungsgründe. Wenn Sie darauf aus sind, zu schockieren und zu beleidigen, dann ist der App Store nicht der richtige Ort für Ihre App.
Einige dieser Regeln sind auch in den Richtlinien für die Beglaubigung von iOS Apps enthalten.

1.1 Anstößige Inhalte

Apps dürfen keine Inhalte umfassen, die beleidigend, unsensibel, verärgernd, ekelerregend, außergewöhnlich geschmacklos oder einfach nur unangenehm sind. Im Folgenden finden Sie einige Beispiele für derartige Inhalte:

1.1.1 Verleumderische, diskriminierende oder böswillige Inhalte, einschließlich Bemerkungen oder Kommentare zu Religion, ethnischer Herkunft, sexueller Orientierung, Geschlecht, nationaler Herkunft oder anderer gezielter Angriffe gegen bestimmte Gruppen, besonders in Fällen, in denen absehbar ist, dass die App eine Zielperson oder -gruppe bloßstellen, einschüchtern oder gefährden wird. Von Berufs wegen politische Satiriker und Humoristen sind im Allgemeinen von dieser Bestimmung ausgenommen.

1.1.2 Realistische Darstellungen von Menschen oder Tieren, die getötet, verstümmelt, gefoltert oder misshandelt werden, oder Inhalte, die Gewalt fördern. Bei „Feinden" im Kontext eines Spiels darf es sich nicht ausschließlich um Menschen einer bestimmten Hautfarbe, Kultur, real existierenden Regierung, eines echten Unternehmens oder um eine andere reale Person handeln.

1.1.3 Darstellungen, die den rechtswidrigen oder rücksichtslosen Einsatz von Waffen und gefährlichen Gegenständen fördern oder den Kauf von Schusswaffen oder Munition erleichtern.

1.1.4 Offensichtlich sexuelles oder pornografisches Material, definiert als „explizite Beschreibungen oder Darstellungen von Geschlechtsorganen oder Aktivitäten, die eher erotische als ästhetische oder emotionale Gefühlen erregen sollen". Dazu gehören „Dating"-Apps und andere Apps, die Pornografie enthalten oder verwendet werden können, um Prostitution oder Menschenhandel und Ausbeutung zu erleichtern.

1.1.5 Provozierende religiöse Kommentare oder ungenaue oder irreführende Zitate religiöser Texte.

1.1.6 🔑 Falsche Informationen und Features, darunter ungenaue Gerätedaten oder Trick-/Witzfunktionen wie z. B. eine falsche Standortverfolgung. Durch die Aussage, dass die App „zu Unterhaltungszwecken" dient, wird diese Richtlinie nicht umgangen. Apps, die anonyme oder scherzhafte Anrufe oder SMS/MMS ermöglichen, werden abgelehnt.

1.1.7 Schädliche Konzepte, die einen Nutzen aus aktuellen oder kürzlichen Ereignissen wie gewaltsamen Konflikten, Terroranschlägen und Epidemien ziehen oder davon profitieren.

1.2 Nutzergenerierte Inhalte

Apps mit nutzergenerierten Inhalten stellen besondere Herausforderungen dar, die von Verletzungen des geistigen Eigentums bis hin zu anonymem Mobbing reichen. Um Missbrauch vorzubeugen, müssen Apps mit von Nutzer:innen erstellten Inhalten oder mit Diensten für soziale Netzwerke Folgendes bieten:

- Eine Filtermethode, um zu verhindern, dass anstößiges Material in der App veröffentlicht wird
- Ein Mechanismus zum Melden anstößiger Inhalte und zeitnahe Reaktionen auf Bedenken
- Die Möglichkeit, missbräuchliche Nutzer:innen für den Service zu sperren
- Öffentlich verfügbare Kontaktdaten, sodass Nutzer:innen Sie leicht erreichen können

Apps mit von Nutzer:innen erstellten Inhalten oder Diensten, die letztendlich primär für pornografische Inhalte, Chatroulette-ähnliche Erfahrungen, die Objektivierung realer Personen (z. B. Abstimmungen bezüglich ihrer Attraktivität), Androhung physischer Gewalt oder Mobbing dienen, sind im App Store fehl am Platz und können ohne Ankündigung entfernt werden. Wenn Ihre App nutzergenerierte Inhalte von einem webbasierten Service enthält, dürfen darin gelegentlich nicht jugendfreie „NSFW"-Inhalte angezeigt werden, sofern diese standardmäßig ausgeblendet sind und nur angezeigt werden, wenn Nutzer:innen sie über Ihre Website aktivieren.

1.2.1 Creator-Inhalte

Apps, die Inhalte einer bestimmten Community von Nutzer:innen namens „Creator" enthalten, stellen eine große Chance dar, wenn sie richtig moderiert werden. Diese Apps bieten Kund:innen ein einzigartiges, einheitliches Erlebnis, um mit verschiedenen Arten von Videoinhalten zu interagieren. Mit Tools und Programmen unterstützen sie diese Community von Nichtentwickler:innen dabei, nutzergenerierte Erlebnisse zu erstellen, zu teilen und zu monetarisieren. Diese Erlebnisse dürfen die Grundfunktion der nativen App nicht verändern, sondern ergänzen diese strukturierte Erlebnisse mit Inhalten. Diese Erlebnisse sind keine nativen „Apps", die von Entwickler:innen programmiert werden, sondern Inhalte in der App selbst. Von App Review werden sie wie nutzergenerierte Inhalte behandelt. Solche Creator-Inhalte können Videos, Artikel, Audioinhalte und sogar einfache Spiele umfassen. Apps, die solche nutzergenerierten Inhalte anbieten, dürfen im App Store veröffentlicht werden, solange sie alle Richtlinien einhalten, einschließlich Richtlinie 1.2 zur Moderation nutzergenerierter Inhalte und Richtlinie 3.1.1 zu Zahlungen und In-App-Käufen. Creator-Apps müssen die Altersfreigabe der Creator-Inhalte mit der höchsten Altersbeschränkung enthalten und die Nutzer:innen darüber informieren, welche Inhalte zusätzliche Käufe erfordern.

1.3 Kategorie „Kinder"

Die Kategorie „Kinder" ist eine einfache Möglichkeit, Apps zu finden, die für Kinder entwickelt wurden. Wenn Sie Inhalte in der Kategorie „Kinder" veröffentlichen möchten, sollten Sie sich darauf konzentrieren, gerade jüngeren Nutzer:innen ein tolles Erlebnis zu bieten. Apps dieser Art dürfen keine Links zu Inhalten außerhalb der App, keine Kaufoptionen oder weitere Ablenkungen für Kinder enthalten, es sei denn, sie befinden sich ausschließlich in Abschnitten der App, die Kontrollfunktionen für Eltern bieten. Denken Sie daran, dass Ihre App die Anforderungen der Kategorie „Kinder" auch in späteren Updates erfüllen muss, auch wenn Sie die Auswahl der Kategorie aufheben. Erfahren Sie mehr über Kontrollfunktionen für Eltern.

Sie müssen die weltweit geltenden Datenschutzgesetze in Bezug auf die Onlinesammlung von Daten von Kindern einhalten. Weitere Informationen finden Sie im Abschnitt Datenschutz dieser Richtlinien. Darüber hinaus dürfen Apps der Kategorie „Kinder" keine personenbezogenen Daten oder Gerätedaten an Dritte senden. Apps in der Kategorie „Kinder" dürfen keine Analysen oder Werbung von Dritten enthalten. Das ermöglicht ein sichereres Erlebnis für Kinder. In wenigen Fällen sind Analysen von Dritten möglicherweise erlaubt, vorausgesetzt, dass die Dienste nicht den IDFA oder beliebige identifizierbare Informationen über Kinder (wie Name, Geburtsdatum, E-Mail-Adresse), Standort oder Geräte erfassen oder übermitteln. Dazu gehören alle Geräte- und Netzwerkdaten sowie weiteren Informationen, die direkt oder in Kombination mit anderen Informationen verwendet werden könnten, um Nutzer:innen und ihre Geräte zu identifizieren. In bestimmten Fällen ist auch kontextbezogene Werbung von Dritten zulässig, sofern die Dienste öffentlich dokumentierte Vorgehensweisen und Richtlinien für Apps der Kategorie „Kinder" umfassen, die eine menschliche Überprüfung der Anzeigen auf Altersgerechtigkeit beinhalten.

1.4 Körperliche Schäden

Wenn sich Ihre App so verhält, dass sie möglicherweise körperliche Schäden verursacht, können wir sie ablehnen. Beispiel:

1.4.1 Medizinische Apps, die ungenaue Daten oder Informationen bereitstellen oder zur Diagnose oder Behandlung von Patient:innen verwendet werden könnten, werden möglicherweise gründlicher überprüft.

• Die von der App genutzten Daten und angewandten Methoden müssen klar dargelegt werden, um nachzuweisen, dass gesundheitsbezogene Messungen so genau wie angegeben durchgeführt werden können. Wenn Genauigkeit oder Verlässlichkeit der Methoden nicht belegt werden können, wird Ihre App abgelehnt. Zum Beispiel sind keine Apps zulässig, die laut eigener Angabe nur über die Sensoren des Geräts Röntgenaufnahmen erstellen oder den Blutdruck, die Körpertemperatur, den Blutzuckerspiegel oder den Sauerstoffgehalt im Blut messen.

• Apps müssen Nutzer:innen daran erinnern, zusätzlich zur Nutzung der App und vor dem Treffen medizinischer Entscheidungen einen Arzt oder eine Ärztin zu konsultieren.

Wenn Ihre medizinische App die behördliche Freigabe erhalten hat, müssen Sie über Ihre App einen Link zu dieser Dokumentation bereitstellen.

1.4.2 Rechner zur Arzneimitteldosierung müssen vom Arzneimittelhersteller, einem Krankenhaus, einer Universität, einer Krankenkasse, einer Apotheke oder einer anderen zugelassenen Einrichtung stammen oder von der FDA oder einer internationalen vergleichbaren Einrichtung genehmigt werden. Angesichts der potenziellen Gefahren, die solche Apps für Patient:innen darstellen können, müssen wir uns darauf verlassen können, dass die App langfristig unterstützt wird und dass Updates für sie bereitgestellt werden.

1.4.3 Apps, die den Konsum von Tabak- und Vape-Produkten, illegalen Drogen oder übermäßigen Mengen Alkohol fördern, sind nicht erlaubt. Apps, die Minderjährige zum Konsum dieser Substanzen ermutigen, werden abgelehnt. Die Erleichterung des Verkaufs von kontrollierten Substanzen (mit Ausnahme lizenzierter Apotheken und lizenzierter oder anderweitig zugelassener Cannabis-Ausgabestellen) oder Tabak ist nicht gestattet.

1.4.4 Apps dürfen nur DUI Checkpoints anzeigen, die von Strafverfolgungsbehörden veröffentlicht wurden, und dürfen niemals betrunkenes Fahren oder andere rücksichtslose Verhaltensweisen wie z. B. überhöhte Geschwindigkeit fördern.

1.4.5 Apps dürfen Kund:innen nicht dazu ermutigen, an Aktivitäten (etwa Wetten, Herausforderungen usw.) teilzunehmen oder ihre Geräte so zu verwenden, dass sie sich selbst oder anderen körperlichen Schaden zufügen können.

1.5 Entwicklerinformationen

Die Nutzer:innen müssen wissen, wie sie Sie bei Fragen und Problemen erreichen können. Stellen Sie sicher, dass Ihre App und die Support-URL eine einfache Möglichkeit enthalten, mit Ihnen Kontakt aufzunehmen. Das ist besonders wichtig für Apps, die möglicherweise im Unterricht verwendet werden. Das Fehlen korrekter und aktueller Kontaktdaten frustriert Kund:innen nicht nur, sondern verstößt

außerdem unter Umständen in einigen Ländern oder Regionen gegen Gesetze. Stellen Sie außerdem sicher, dass Wallet-Karten gültige Kontaktdaten des Ausstellers enthalten und mit einem speziellen Zertifikat signiert sind, das dem Inhaber des Warenzeichens oder der Marke zugeordnet ist.

1.6 Datensicherheit

Für die Apps müssen angemessene Sicherheitsmaßnahmen implementiert werden, um den ordnungsgemäßen Umgang mit Nutzerdaten zu gewährleisten, die gemäß der Lizenzvereinbarung für das Apple Developer Program und diesen Richtlinien gesammelt wurden (weitere Informationen siehe Richtlinie 5.1), und ihre unbefugte Nutzung, Offenlegung oder den Zugriff durch Dritte zu verhindern.

1.7 Meldung krimineller Aktivitäten

Apps zur Meldung mutmaßlicher krimineller Aktivitäten müssen die örtlichen Strafverfolgungsbehörden einbeziehen und dürfen nur in Ländern oder Regionen angeboten werden, in denen eine solche Einbeziehung aktiv stattfindet.

---

2. Leistung

2.1 Vollständigkeit der App

Bei Apps, die bei App Review eingereicht werden, einschließlich Apps, die Sie zur Vorbestellung zur Verfügung stellen, muss es sich um endgültige Versionen mit allen erforderlichen Metadaten und voll funktionsfähigen URLs handeln. Platzhaltertext, leere Websites und andere temporäre Inhalte müssen vor dem Einreichen gelöscht werden. Prüfen Sie Ihre App vor dem Einreichen auf einem Gerät auf Fehler und Stabilitätsprobleme und reichen Sie mit der App auch die Anmeldedaten für einen Demoaccount ein (und aktivieren Sie Ihren Backend-Dienst), wenn Ihre App eine Anmeldevorgang umfasst. Wenn Sie aufgrund von rechtlichen oder sicherheitstechnischen Verpflichtungen keinen Demoaccount bereitstellen können, können Sie mit vorheriger Einwilligung von Apple einen integrierten Demomodus anstelle eines Demoaccounts verwenden. Stellen Sie sicher, dass in diesem Demomodus alle Features und Funktionen Ihrer App zu sehen sind. Wenn Sie In-App-Käufe in Ihrer App anbieten, achten Sie darauf, dass diese vollständig, aktuell und für den Prüfer sichtbar sind, oder erläutern Sie in den Notizen, warum dies nicht der Fall ist. Nutzen Sie App Review nicht als Softwaretestservice. Wir lehnen unvollständige App-Pakete und -Binärdateien ab, die abstürzen oder offensichtliche technische Probleme aufweisen.

2.2 Betatests

Demos, Betaversionen und Testversionen Ihrer App gehören nicht in den App Store – verwenden Sie hierfür stattdessen TestFlight. Betaversionen von Apps, die zur Verteilung über TestFlight eingereicht werden, müssen zur Veröffentlichung bestimmt sein und die App Review Richtlinien erfüllen. Beachten Sie jedoch, dass für Apps, die via TestFlight an Tester:innen verteilt werden, jegliche Vergütung unzulässig ist. Dies schließt auch die Belohnung für die Teilnahme an einer Crowdfunding-Kampagne mit

ein. Wichtige Updates für Ihre Betaversion müssen vor der Verteilung an die Tester:innen zunächst bei App Review für TestFlight eingereicht werden. Weitere Informationen finden Sie auf der Seite zu Betatests in TestFlight.

2.3 Genaue Metadaten

Kund:innen müssen wissen, was sie beim Laden oder Kaufen Ihrer App bekommen. Achten Sie also darauf, dass alle App-Metadaten, einschließlich der Datenschutzinformationen, App-Beschreibung, Bildschirmfotos und Vorschauen, das Kernerlebnis in der App genau widerspiegeln, und halten Sie sie mit neuen Versionen auf dem neuesten Stand.

2.3.1

(a) Binden Sie keine verborgenen, ruhenden oder undokumentierten Features in Ihre App ein. Die Funktionalität Ihrer App muss für Endnutzer:innen und App Review klar ersichtlich sein. Alle neuen Features, Funktionen und Produktänderungen müssen in den Notizen für App Review in App Store Connect genau beschrieben werden (generische Beschreibungen werden abgelehnt) und zugänglich sein. Ebenso stellen die irreführende Vermarktung Ihrer App, z. B. durch Werbung für Inhalte oder Dienste, die sie nicht wirklich anbietet (etwa auf iOS basierende Viren- und Malwarescanner), und die Bewerbung eines falschen Preises, ob innerhalb oder außerhalb des App Store, Gründe für die Entfernung Ihrer App aus dem App Store oder die Sperrung einer Installation über die alternative Verteilung und die Kündigung Ihres Entwickleraccounts dar.

(b) Besonders schwerwiegende oder wiederholte Verhaltensweisen stellen einen Grund für die Entfernung aus dem Apple Developer Program dar. Wir arbeiten hart daran, dass der App Store eine vertrauenswürdige Plattform ist und bleibt, und erwarten von unseren App-Entwickler:innen, dass sie unserem Beispiel folgen. Wir pflegen keine Geschäftsbeziehungen mit unaufrichtigen Personen.

2.3.2 Wenn Ihre App In-App-Käufe enthält, müssen Sie sicherstellen, dass anhand der App-Beschreibung, Bildschirmfotos und Vorschauen klar erkennbar ist, ob vorgestellte Elemente, Levels, Abonnements usw. zusätzliche Käufe erfordern. Wenn Sie sich dafür entscheiden, In-App-Käufe im App Store zu bewerben, müssen Sie sicherstellen, dass der Anzeigename, das Bildschirmfoto und die Beschreibung des In-App-Kaufs für eine öffentliche Zielgruppe geeignet sind, dass die Richtlinien für die Bewerbung für In-App-Käufe eingehalten werden und dass die SKPaymentTransactionObserver-Methode in Ihrer App ordnungsgemäß eingerichtet ist, damit Kund:innen den Kauf nahtlos abschließen können, wenn Ihre App gestartet wird.

2.3.3 Bildschirmfotos müssen die App während der Verwendung zeigen, nicht nur das Titelbild, die Anmeldeseite oder den Begrüßungsbildschirm. Sie können auch Text- und Bildüberlagerungen enthalten (z. B. um Eingabemechanismen wie einen animierten Touchpoint oder einen Apple Pencil zu demonstrieren) und erweiterte Funktionen auf dem Gerät zeigen, etwa die Touch Bar.

2.3.4 Anhand von Vorschauen sehen die Nutzer, wie Ihre App aussieht und welche Funktionen sie umfasst. Damit die Nutzer:innen verstehen, was ihnen Ihre App bietet, dürfen Vorschauen nur Videoaufnahmen der App selbst umfassen. Das Nutzererlebnis in der Nachrichten-App kann durch Sticker und iMessage-Erweiterungen dargestellt werden. Sie können gesprochenen Text und Video- oder Textüberlagerungen hinzufügen, um alles zu erklären, was allein durch das Video nicht klar wird.

2.3.5 Wählen Sie die für Ihre App am besten geeignete Kategorie aus und sehen Sie sich die Definitionen zu App Store-Kategorien, falls Sie dabei Hilfe brauchen. Falls Sie eine ganz abweichende Kategorie festlegen, ändern wir diese möglicherweise für Sie.

2.3.6 Beantworten Sie die Fragen zur Altersfreigabe in App Store Connect ehrlich, damit Ihre App ordnungsgemäß mit der Kindersicherung ausgestattet wird. Eine falsche Bewertung Ihrer App führt möglicherweise dazu, dass die Nutzer:innen von den Inhalten überrascht sind oder eine Anfrage einer staatlichen Behörden ausgelöst wird. Wenn Ihre App Medien enthält, für die Inhaltsbewertungen oder Warnhinweise angezeigt werden müssen (z. B. Filme, Musik, Spiele), sind Sie dafür verantwortlich, dass die lokalen Bestimmungen jedes Gebiets, in dem Ihre App verfügbar ist, eingehalten werden.

2.3.7 Wählen Sie einen eindeutigen App-Namen, weisen Sie Keywords zu, die Ihre App genau beschreiben, und versuchen Sie nicht, in Ihre Metadaten markenrechtlich geschützte Begriffe, beliebte App-Namen, Preisinformationen oder andere irrelevante Ausdrücke zu integrieren, nur um das System zu umgehen. App-Namen dürfen maximal 30 Zeichen lang sein. Metadaten wie App-Namen, Untertitel, Bildschirmfotos und Vorschauen dürfen keine Preise, Begriffe oder Beschreibungen enthalten, die nicht spezifisch für den Metadatentyp sind. App-Untertitel sind eine gute Möglichkeit, zusätzlichen Kontext für Ihre App bereitzustellen. Sie müssen unseren Standardregeln für Metadaten entsprechen und dürfen keine unangemessenen Inhalte enthalten, auf andere Apps verweisen oder unbestätigte Produktansprüche geltend machen. Apple kann unangemessene Keywords jederzeit ändern oder andere geeignete Maßnahmen ergreifen, um Missbrauch zu verhindern.

2.3.8 Die Metadaten müssen für alle Zielgruppen angemessen sein. Stellen Sie also unabhängig davon, ob Ihre App für eine höhere Altersgruppe eingestuft ist, immer sicher, dass die Symbole der App und für In-App-Käufe sowie Bildschirmfotos und Vorschauen für die Altersgruppe 4+ geeignet sind. Wenn es sich bei Ihrer App beispielsweise um ein Spiel handelt, das Gewalt enthält, wählen Sie Bilder aus, die weder einen grausamen Tod noch eine Waffe zeigen, die auf einen bestimmten Charakter gerichtet ist. Die Verwendung von Ausdrücken wie „Für Kinder“ in den App-Metadaten ist im App Store der Kategorie „Kinder“ vorbehalten. Stellen Sie sicher, dass Ihre Metadaten, einschließlich App-Name und Symbole (klein, groß, Apple Watch App, alternative Symbole usw.), ähnlich sind, um Verwirrung zu vermeiden.

2.3.9 Sie sind dafür verantwortlich, die Rechte für die Nutzung aller Materialien in Ihren App-Symbolen, Bildschirmfotos und Vorschauen einzuholen, und Sie sollten fiktive Accountinformationen anstelle von Daten einer echten Person anzeigen.

2.3.10 Achten Sie darauf, dass sich Ihre App auf das Erlebnis in iOS, iPadOS, macOS, tvOS oder watchOS konzentriert, und benutzen Sie keine Namen, Symbole oder Bilder anderer mobiler Plattformen oder alternativer App-Marktplätze in Ihrer App oder Ihren Metadaten, es sei denn, es sind bestimmte, genehmigte interaktive Funktionen vorhanden. Stellen Sie sicher, dass sich Ihre App-Metadaten auf die App selbst und die darin angebotene Erfahrung konzentrieren. Fügen Sie keine irrelevanten Informationen ein.

2.3.11 Apps, die Sie zur Vorbestellung im App Store einreichen, müssen vollständig und wie eingereicht verfügbar sein. Stellen Sie sicher, dass sich die App, die Sie letztendlich veröffentlichen, nicht wesentlich von der Bewerbung der App im Vorbestellungszustand unterscheidet. Wenn Sie wesentliche Änderungen an der App vornehmen (z. B. Geschäftsmodelle ändern), müssen Sie die Vorbestellungen erneut starten.

2.3.12 Neue Features und Produktänderungen müssen in der App im Text zur Ankündigung von Neuigkeiten klar beschrieben werden. Einfache Fehlerbehebungen, Sicherheitsupdates und Leistungsverbesserungen können generisch beschrieben werden, aber wichtigere Änderungen müssen in den Notizen aufgeführt werden.

2.3.13 In-App-Ereignisse sind zeitliche Ereignisse in Ihrer App. Um Ihr Ereignis im App Store zu präsentieren, muss es einem in App Store Connect vorhandenen Ereignistyp zugeordnet sein. Alle Ereignismetadaten müssen korrekt sein und sich auf das Ereignis selbst beziehen, nicht auf die App im Allgemeinen. Ereignisse müssen zu den Zeiten und Daten stattfinden, die Sie in App Store Connect ausgewählt haben, auch über mehrere Store-Seiten hinweg. Sie dürfen ein Ereignis monetarisieren, solange Sie die Regeln zu Geschäften in Abschnitt 3 befolgen. Der Deep-Link für das Ereignis muss Nutzer:innen zum richtigen Ziel in Ihrer App führen. Unter In-App-Ereignisse finden Sie weitere Informationen zu zugelassenen Metadaten und Deep-Links für Ereignisse.

2.4 Hardwarekompatibilität

2.4.1 Um sicherzustellen, dass Nutzer:innen umfassend von Ihrer App profitieren, sollten iPhone Apps nach Möglichkeit auch auf einem iPad ausgeführt werden können. Wir empfehlen Ihnen, universelle Apps zu erstellen, damit die Nutzer:innen sie auf sämtlichen Geräten verwenden können. Erfahren Sie mehr über universelle Apps.

2.4.2 🔑 Entwickeln Sie Ihre App so, dass sie Strom effizient nutzt und verwendet werden kann, ohne das Gerät zu beschädigen. Apps sollten nicht dafür sorgen, dass der Akku schnell entladen wird, übermäßige Wärme erzeugt wird oder die Ressourcen des Geräts übermäßig belastet werden. Apps dürfen beispielsweise nicht dazu animieren, das Gerät während des Ladens unter eine Matratze oder ein Kissen zu legen oder auf dem Solid-State-Drive übermäßig viele Schreibzyklen ausführen. Apps, einschließlich Werbeanzeigen von Dritten, dürfen keine Hintergrundprozesse wie das Mining von Kryptowährungen ausführen.

2.4.3 Die Nutzer:innen sollten in der Lage sein, Ihre Apple TV App ohne zusätzliche Hardwareeingaben, die über die Siri Remote oder Gamecontroller von Dritten hinausgehen, zu nutzen. Für weitere angeschlossene Peripheriegeräte können Sie jedoch erweiterte Funktionen bereitstellen. Wenn Sie einen Gamecontroller verlangen, müssen Sie das in den Metadaten klar erläutern, damit die Nutzer wissen, dass sie zum Spielen zusätzliche Ausrüstung benötigen.

2.4.4 🔑 Apps dürfen niemals einen Neustart des Geräts oder Änderungen an den Systemeinstellungen verlangen oder erfordern, wenn kein Zusammenhang mit der Kernfunktionalität der App besteht. Ermutigen Sie Nutzer:innen beispielsweise nicht, das WLAN auszuschalten, Sicherheitsfunktionen zu deaktivieren usw.

2.4.5 Für Apps, die über den Mac App Store vertrieben werden, gelten einige zusätzliche Anforderungen:

(i) Sie müssen sich in einer geeigneten Sandbox befinden und den Bestimmungen der macOS File System Documentation entsprechen. Darüber hinaus dürfen sie für die Änderung von Nutzerdaten, die von anderen Apps (wie Lesezeichen, Adressbüchern oder Kalendereinträgen) gespeichert werden, nur die entsprechenden macOS-APIs nutzen.

(ii) Sie müssen mit den in Xcode bereitgestellten Technologien verpackt und eingereicht werden. Installationsprogramme von Dritten sind nicht zulässig. Sie müssen in sich geschlossene Installationspakete für einzelne Apps sein und dürfen Code oder Ressourcen nicht an gemeinsam genutzten Standorten installieren.

(iii) Sie dürfen nicht automatisch starten oder anderen Code beim Start oder bei der Anmeldung ohne Zustimmung automatisch ausführen lassen oder Prozesse starten, die ohne Zustimmung weiterlaufen, nachdem ein:e Nutzer:in die App beendet hat. Sie dürfen Symbole nicht automatisch dem Dock hinzufügen oder Verknüpfungen auf dem Desktop der Nutzer:innen erstellen.

(iv) Sie dürfen keine eigenständigen Apps, Kexts, zusätzlichen Code oder Ressourcen laden oder installieren, um Funktionen hinzuzufügen oder die App im Vergleich zum Überprüfungsprozess wesentlich zu verändern.

(v) Sie dürfen keine Rechteausweitung auf Root-Berechtigungen anfordern oder Setuid-Attribute verwenden.

(vi) Sie dürfen beim Start keinen Lizenzbildschirm anzeigen, Lizenzschlüssel verlangen oder einen eigenen Kopierschutz implementieren.

(vii) Sie müssen Updates über den Mac App Store bereitstellen. Andere Mechanismen für Updates sind nicht zulässig.

(viii) Apps müssen auf dem derzeit ausgelieferten Betriebssystem ausgeführt werden und dürfen keine veralteten oder optional installierten Technologien (z. B. Java) verwenden.

(ix) Apps müssen die gesamte Sprach- und Lokalisierungsunterstützung in einem einzigen App-Paket beinhalten.

2.5 Softwarevoraussetzungen

2.5.1 Apps dürfen nur öffentliche APIs verwenden und müssen auf dem derzeit ausgelieferten Betriebssystem ausgeführt werden. Erfahren Sie mehr über öffentliche APIs. Halten Sie Ihre Apps auf dem neuesten Stand und stellen Sie sicher, dass Sie alle veralteten Features, Frameworks oder Technologien auslaufen lassen, die in zukünftigen Versionen des Betriebssystems nicht mehr unterstützt werden. Apps müssen APIs und Frameworks für die beabsichtigten Zwecke verwenden und diese Integration in der App-Beschreibung angeben. So sollte das HomeKit Framework beispielsweise ausschließlich für Dienste zur Heimautomatisierung verwendet und das HealthKit nur im Bereich Gesundheit und Fitness eingesetzt und in die Health App eingebunden werden.

2.5.2 Apps müssen in den jeweiligen Paketen in sich geschlossen sein und dürfen weder Daten außerhalb des festgelegten Containerbereichs lesen oder schreiben noch Code laden, installieren oder ausführen, der Features oder Funktionen der App, einschließlich anderer Apps, einführt oder ändert. Apps für das Bildungswesen, die zum Unterrichten, Entwickeln oder Testen von ausführbarem Code entwickelt wurden, dürfen unter bestimmten Umständen Code laden, sofern dieser nicht für andere Zwecke verwendet wird. Derartige Apps müssen den von der App bereitgestellten Quellcode für die Nutzer:innen vollständig sichtbar und bearbeitbar bereitstellen.

2.5.3 Apps, die Viren, Dateien, Computercode oder Programme übertragen, die den normalen Betrieb des Betriebssystems und/oder der Hardwarefeatures beeinträchtigen oder stören könnten, einschließlich Push-Mitteilungen und Game Center, werden abgelehnt. Besonders schwerwiegende Verstöße und wiederholte Verhaltensweisen führen zur Entfernung aus dem Apple Developer Program.

2.5.4 Multitasking-Apps dürfen Hintergrunddienste nur für die dafür vorgesehenen Zwecke nutzen: VoIP, Audiowiedergabe, Standortabfrage, Erledigung von Aufgaben, lokale Benachrichtigungen usw.

2.5.5 Apps müssen in reinen IPv6-Netzwerken voll funktionsfähig sein.

2.5.6 In Apps, die das Surfen im Internet ermöglichen, müssen das entsprechende WebKit Framework und WebKit JavaScript verwendet werden. Sie können eine Berechtigung zur Verwendung einer alternativen Webbrowser-Engine in Ihrer App beantragen. Erfahren Sie mehr über diese Berechtigungen.

2.5.7 Absichtlich ausgelassen.

2.5.8 Apps, die alternative Desktop-/Homescreen-Umgebungen erstellen oder Erfahrungen über ein Multi-App-Widget simulieren, werden abgelehnt.

2.5.9 Apps, die die Funktionsweise von Standardschaltern wie z. B. den Schaltern „Lauter/Leiser“ und „Klingeln/Aus“ oder andere Elemente oder Verhaltensweisen der nativen Benutzeroberfläche ändern oder deaktivieren, werden abgelehnt. Zum Beispiel dürfen Apps keine Links zu anderen Apps oder Features blockieren, von denen Nutzer:innen erwarten, dass sie auf eine bestimmte Weise funktionieren.

2.5.10 Apps dürfen nicht mit leeren Werbebannern oder Testanzeigen eingereicht werden.

2.5.11 SiriKit und Kurzbefehle

> **(i)** Apps, die SiriKit und Kurzbefehle integrieren, dürfen nur für Zwecke registriert werden, für die sie ohne Unterstützung einer zusätzlichen App geeignet sind und die Nutzer:innen anhand der angegebenen Funktionalität erwarten würden. Wenn es sich bei Ihrer App beispielsweise eine App zur Essensplanung handelt, sollten Sie nicht den Zweck integrieren, ein Training zu starten, auch wenn die App mit einer Fitness-App integriert werden kann.
>
> **(ii)** Stellen Sie sicher, dass das Vokabular und die Ausdrücke in Ihrer .plist-Datei der App und der Siri-Funktionalität der Zwecke entsprechen, für die die App registriert ist. Aliasse müssen sich direkt auf den Namen Ihrer App oder Ihres Unternehmens beziehen und dürfen keine generischen Begriffe sein oder App-Namen oder -Dienste von Dritten enthalten.

(iii) Bearbeiten Sie die Siri-Anfrage oder den Kurzbefehl so geradlinig wie möglich und fügen Sie keine Anzeigen oder andere Marketingmaßnahmen zwischen der Anfrage und Bearbeitung ein. Fordern Sie eine Begriffserklärung nur an, wenn dies zum Erledigen der Aufgabe erforderlich ist (z. B. Nutzer:innen bitten, genauere Angaben zu einer bestimmten Art von Training zu machen).

2.5.12 Apps, die CallKit verwenden oder eine Erweiterung gegen betrügerische SMS-Nachrichten enthalten, dürfen nur Telefonnummern sperren, über die bekanntermaßen Spam versendet wird. Wenn Apps Funktionen zum Blockieren von Anrufen, SMS und MMS oder zur Identifizierung von Spam enthalten, müssen diese Features im Marketingtext eindeutig angegeben sein und die Kriterien für Sperr- und Spam-Listen müssen aufgeführt werden. Sie dürfen die Daten, auf die über diese Tools zugegriffen wird, nicht für Zwecke verwenden, die nicht unmittelbar mit dem Betrieb oder der Verbesserung Ihrer App oder Erweiterung zusammenhängen (z. B. dürfen Sie sie nicht zu Trackingzwecken verwenden, teilen oder verkaufen, damit Nutzerprofile erstellen usw.).

2.5.13 Apps, die zur Accountauthentifizierung Gesichtserkennung einsetzen, müssen nach Möglichkeit LocalAuthentication (nicht ARKit oder eine andere Gesichtserkennungstechnologie) verwenden und für Nutzer:innen unter 13 Jahren eine alternative Authentifizierungsmethode einsetzen.

2.5.14 Apps müssen bei der Aufnahme, Protokollierung oder anderweitigen Aufzeichnung von Nutzeraktivitäten die ausdrückliche Zustimmung der Nutzer:innen einholen und deutlich visuell und/oder akustisch darauf hinweisen. Das schließt die Verwendung der Kamera, des Mikrofons, der Bildschirmaufnahmen oder anderer Nutzereingaben ein.

2.5.15 Apps, mit denen Nutzer:innen Dateien anzeigen und auswählen können, sollten Elemente aus der Dateien-App und den iCloud-Dokumenten der Nutzer:innen enthalten.

2.5.16 Widgets, Erweiterungen und Benachrichtigungen müssen sich auf den Inhalt und die Funktionsweise Ihrer App beziehen.

(a) Darüber hinaus müssen alle Features und Funktionen von App Clips in der Hauptbinärdatei der App enthalten sein. App Clips dürfen keine Werbung enthalten.

2.5.17 Apps, die Matter unterstützen, müssen das Support-Framework von Apple für Matter verwenden, damit die Kopplung gestartet werden kann. Wenn Sie in Ihrer App eine andere Matter-Softwarekomponente als das von Apple bereitgestellte Matter SDK verwenden, muss diese Softwarekomponente durch die Connectivity Standards Alliance für die jeweilige Plattform zertifiziert sein.

2.5.18 Displaywerbung muss auf die Hauptbinärdatei der App beschränkt sein und darf nicht in Erweiterungen, App Clips, Widgets, Mitteilungen, Tastaturen, watchOS Apps usw. enthalten sein. Anzeigen, die in einer App zu sehen sind, müssen für die Altersfreigabe der App geeignet sein, den Nutzer:innen ermöglichen, alle Informationen zu sehen, die verwendet werden, um diese Anzeige für ihn zu personalisieren (ohne dass die Nutzer:innen die App verlassen müssen), und dürfen keine personalisierte oder verhaltensabhängige Werbung auf Grundlage sensibler Nutzerdaten wie Gesundheits-/medizinischen Daten (z. B. aus den HealthKit APIs), Daten aus Schule und Unterricht (z. B. aus ClassKit) oder von Kindern (z. B. aus Apps in der Kategorie „Kinder“ im App Store) usw. umfassen. Interstitial-Anzeigen oder Anzeigen, die das Nutzererlebnis unterbrechen oder blockieren,

müssen klar als Werbung erkennbar sein, dürfen Nutzer:innen nicht manipulieren oder verleiten, darauf zu tippen, und müssen einfach zugängliche und sichtbare Tasten zum Schließen/Überspringen bereitstellen, die groß genug zum Verwerfen der Werbung sind. Apps, die Werbung enthalten, müssen den Nutzer:innen auch die Möglichkeit bieten, unangemessene oder nicht altersgemäße Werbung zu melden.

---

3. Geschäfte

Sie haben verschiedene Möglichkeiten, Ihre App im App Store zu monetarisieren. Wenn Ihr Geschäftsmodell nicht offensichtlich ist, sollten Sie es in den Metadaten und in den Notizen für App Review erläutern. Wenn wir nicht nachvollziehen können, wie Ihre App funktioniert oder Ihre In-App-Käufe nicht unmittelbar klar werden, verzögert das die Überprüfung und zieht möglicherweise eine Ablehnung nach sich. Zwar dürfen Sie die Preise selbst festlegen, doch wir verteilen keine Apps und In-App-Käufe, bei denen es sich klar um Abzocke handelt. Wir lehnen teure Apps ab, die Nutzer:innen mit unverhältnismäßig hohen Preisen zu betrügen versuchen.

Sollte sich herausstellen, dass Sie versucht haben, die Bewertungen zu manipulieren oder Ihr Ranking zu verbessern, indem Sie für Feedback bezahlt oder andere Anreize geboten, Feedback gefälscht oder gefiltert oder eine dritte Partei zu diesem Zweck beauftragt haben, werden wir Schritte zum Schutz der Integrität des App Store einleiten. Einer dieser Schritte kann der Entzug Ihrer Teilnahmeberechtigung für das Apple Developer Program sein.

3.1 Zahlungen

3.1.1 In-App-Käufe

- Wenn Sie Features oder Funktionen in Ihrer App freischalten möchten (z. B. Abonnements, In-Game-Währungen, Spielelevels, Zugriff auf Premiuminhalte oder das Freischalten einer Vollversion), müssen Sie In-App-Käufe verwenden. Apps dürfen die integrierten Mechanismen nicht verwenden, um Inhalte oder Funktionen wie Lizenzschlüssel, Augmented-Reality-Marker, QR-Codes, Kryptowährungen und Wallets für Kryptowährungen zu entsperren.

- In Apps dürfen In-App-Kaufwährungen verwendet werden, um es Kund:innen zu ermöglichen, den Entwickler:innen oder Anbietern digitaler Inhalte in der App ein „Trinkgeld“ zu geben.

- Guthaben oder In-Game-Währungen, die über In-App-Käufe erworben werden, dürfen nicht ablaufen. Vergewissern Sie sich, dass Sie über einen Wiederherstellungsmechanismus für alle wiederherstellbaren In-App-Käufe verfügen.

- Apps können es ermöglichen, Elemente, die für In-App-Käufe infrage kommen, an andere zu verschenken. Derartige Geschenke können nur dem ursprünglichen Käufer erstattet und nicht umgetauscht werden.

- In Apps, die über den Mac App Store verteilt werden, können Plug-Ins oder Erweiterungen gehostet werden, die mit anderen Mechanismen als dem App Store aktiviert sind.

- Apps, die „Lootboxen“ oder andere Mechanismen umfassen, in denen randomisierte virtuelle Elemente zum Kauf bereitgestellt werden, müssen Kund:innen vor dem Kauf über die Chancen informieren, die jeweilige Art von Element zu erhalten.

- Digitale Geschenkkarten, Zertifikate, Gutscheine und Coupons, die für digitale Waren oder Dienste eingelöst werden, können in Ihrer App nur über In-App-Käufe verkauft werden. Bei physischen Geschenkkarten, die in einer App verkauft und dann an Kund:innen gesendet werden, sind andere Zahlungsmethoden als In-App-Käufe möglich.

- Apps ohne Abonnement bieten möglicherweise eine kostenlose zeitbasierte Testversion, bevor eine Option zum vollständigen Freischalten angeboten wird. Hierfür wird ein nicht verwendbares IAP-Element auf Preisstufe 0 eingerichtet, das der Namenskonvention „XX-tägige Testversion“ folgt. Vor Beginn der Testphase müssen in Ihrer App eindeutig die Dauer und die Inhalte bzw. Dienste angegeben werden, auf die am Ende der Testphase nicht mehr zugegriffen werden kann, sowie alle Folgegebühren, die Nutzer:innen für die gesamte Funktionalität bezahlen müssten. Erfahren Sie mehr über die Verwaltung des Zugriffs auf Inhalte und die Dauer der Testversion mit Receipts und Device Check.

- Apps dürfen In-App-Käufe verwenden, um Dienste im Zusammenhang mit Non-Fungible Tokens (NFTs) zu verkaufen, z. B. Minting, Listing und Übertragung. Apps dürfen es Nutzer:innen ermöglichen, ihre eigenen NFTs einzusehen, vorausgesetzt, mittels der NFT-Eigentumsrechte werden keine Features oder Funktionen innerhalb der App freigeschaltet. Apps dürfen es Nutzer:innen ermöglichen, NFT-Kollektionen anderer zu durchsuchen, sofern die Apps keine Tasten, externen Links oder andere Handlungsaufforderungen enthalten, die Kund:innen zu anderen Kaufmechanismen als zu In-App-Käufen führen.

3.1.1(a) Link zu anderen Kaufmethoden

Entwickler:innen können Berechtigungen beantragen, in ihrer App einen Link zu einer Website bereitzustellen, für die der:die Entwickler:in verantwortlich ist oder die er:sie betreibt, um digitale Inhalte oder Services zu kaufen. Bitte beachten Sie die weiteren Details unten.

- Berechtigungen für externe StoreKit-Kauflinks: Apps im App Store in bestimmten Regionen bieten möglicherweise In-App Käufe an und nutzen außerdem eine Berechtigung für externe StoreKit-Kauflinks, um einen Link zur Website des:der Entwickler:in einzufügen, der Benutzer:innen über andere Möglichkeiten zum Kauf digitaler Waren oder Diensten informiert. Erfahren Sie mehr über diese Berechtigungen. In Übereinstimmung mit den Berechtigungsvereinbarungen kann der Link die Nutzer:innen darüber informieren, wo und wie sie diese In-App-Artikel kaufen können und dass diese Artikel möglicherweise zu einem vergleichsweise niedrigeren Preis verfügbar sind. Die Berechtigungen sind auf die Nutzung im iOS oder iPadOS App Store in bestimmten Storefronts beschränkt. In allen anderen Storefronts dürfen Apps und ihre Metadaten keine Tasten, externen Links oder anderen Handlungsaufforderungen enthalten, die Kund:innen zu anderen Kaufmechanismen als zu In-App-Käufen führen.

- Berechtigungen für Musikstreamingdienste: Musikstreaming-Apps in bestimmten Regionen können Berechtigungen für Musikstreamingdienste nutzen, um einen Link (in Form einer Taste „Kaufen“) zur Website des:der Entwickler:in einzubinden, der Benutzer:innen über weitere Möglichkeiten zum Kauf digitaler Musikinhalte oder -dienste informiert. Diese Berechtigungen ermöglichen es Entwickler:innen von Musikstreaming-Apps auch, Benutzer:innen zur Angabe ihrer E-Mail-Adresse zu bewegen, speziell damit ihnen ein Link zur Website des:der Entwickler:in gesendet werden kann, über den sie digitale Musikinhalte oder -dienste kaufen können. Erfahren Sie mehr über diese Berechtigungen. In Übereinstimmung mit den Berechtigungsvereinbarungen kann der Link die Nutzer:innen darüber informieren, wo und wie sie diese In-App-Artikel kaufen können und wie hoch der Preis für diese Artikel ist. Die Berechtigungen sind auf die Nutzung im iOS oder iPadOS App Store in bestimmten Storefronts beschränkt. In allen anderen Storefronts dürfen Apps zum Musikstreamen und ihre Metadaten keine Tasten, externen Links oder anderen Handlungsaufforderungen enthalten, die Kund:innen zu anderen Kaufmechanismen als zu In-App-Käufen führen.

- Wenn Ihre App irreführende Marketing-Praktiken, Betrug oder Betrug in Bezug auf die Berechtigung anwendet, wird Ihre App gegebenenfalls aus dem App Store entfernt und Sie werden möglicherweise aus dem Apple Developer Program verwiesen.

3.1.2 Abonnements

Apps dürfen automatisch verlängerbare In-App-Käufe unabhängig von der Kategorie im App Store anbieten. Beim Integrieren automatisch verlängerbarer Abonnements in Ihre App müssen Sie die folgenden Richtlinien befolgen.

3.1.2 (a) Zulässige Verwendungen

Wenn Sie ein automatisch verlängerbares Abonnement anbieten, müssen Sie Kund:innen einen dauerhaften Mehrwert bieten. Der Abonnementzeitraum muss mindestens sieben Tage betragen und auf allen Geräten der Nutzer:innen verfügbar sein. Die folgende Liste ist nicht vollständig, enthält aber einige Beispiele für geeignete Abonnements: neue Spiellevels; episodische Inhalte, Multiplayer-Unterstützung, Apps mit konsistenten inhaltlichen Updates, Zugriff auf große Sammlungen ständig aktualisierter Medieninhalte, Software as a Service („SAAS“) und Cloud-Support. Außerdem muss Folgendes gegeben sein:

- Abonnements dürfen zusätzlich zu frei zusammenstellbaren Angeboten offeriert werden (z. B. können Sie ein Abonnement für eine ganze Bibliothek von Filmen zusätzlich zum Kauf oder Verleih eines einzelnen Films anbieten).

- Sie können ein einzelnes Abonnement anbieten, das Sie für Ihre eigenen Apps und Dienste nutzen.

- Bei Spielen, die im Rahmen eines Abonnements für Streaming-Spiele angeboten werden, darf ein einzelnes Abonnement über alle Apps und Dienste von Dritten hinweg angeboten werden. Sie müssen jedoch direkt aus dem App Store geladen werden, so gestaltet sein, dass doppelte Zahlungen durch Abonnent:innen vermieden werden, und dürfen Kund:innen ohne Abonnement nicht benachteiligen.

- Abonnements müssen auf allen Geräten der Nutzer:innen funktionieren, auf denen die App verfügbar ist. Erfahren Sie mehr über das Anbieten eines Abonnements über mehrere Apps hinweg.

- Apps dürfen die Nutzer:innen nicht dazu zwingen, die App zu bewerten, zu überprüfen, andere Apps herunterzuladen oder ähnliche Aktionen auszuführen, um Zugriff auf Funktionen, Inhalte oder die Nutzung der App zu erhalten.

- Wie für alle Apps gilt auch für Apps mit Abonnementangebot, dass Nutzer:innen die von ihnen erworbenen Optionen nutzen können müssen, ohne vorher weitere Schritte wie z. B. die Veröffentlichung eines Beitrags in einem sozialen Netzwerk, das Hochladen von Kontakten oder mehrmaliges Anmelden bei der App durchführen zu müssen.

- Abonnements dürfen Verbrauchsguthaben, Edelsteine, Spielwährungen usw. umfassen und Sie können Abonnements anbieten, die den Zugang zu ermäßigten Verbrauchsgütern beinhalten (z. B. eine Platinmitgliedschaft, mit der Edelsteinpacks zu einem reduzierten Preis verfügbar sind).

- Wenn Sie eine vorhandene App auf ein abonnementbasiertes Geschäftsmodell umstellen, dürfen Sie keine primäre Funktionalität entfernen, für die bestehende Nutzer:innen bereits bezahlt haben. Lassen Sie beispielsweise Kund:innen, die bereits eine „Vollversion“ eines Spiels freigeschaltet haben, weiterhin auf das vollständige Spiel zugreifen, nachdem Sie ein Abonnementmodell für Neukund:innen eingeführt haben.

- Automatisch verlängerbare Apps dürfen für Kund:innen eine kostenlose Testversion anbieten, indem die entsprechenden in App Store Connect aufgeführten Informationen bereitgestellt werden. Erfahren Sie mehr über das Bereitstellen von Abonnementangeboten.

- Apps, mit denen versucht wird, Nutzer:innen zu betrügen, werden aus dem App Store entfernt. Dazu gehören Apps, die unter Vorspiegelung falscher Tatsachen versuchen, Nutzer:innen zum Abschließen eines Abonnements zu bewegen, oder die Lockvogeltaktiken oder Betrugsmethoden anwenden. Diese werden aus dem App Store entfernt und Sie können aus dem Apple Developer Program entfernt werden.

- Mobilfunkanbieter-Apps dürfen nach vorheriger Einwilligung von Apple automatisch verlängerbare Musik- und Videoabonnements umfassen, die in Paketen mit neuen Mobildatenverträgen gekauft wurden. Andere automatisch verlängerbare Abonnements dürfen nach vorheriger Einwilligung von Apple ebenfalls in Paketen enthalten sein, die mit neuen Mobildatenverträgen gekauft wurden, sofern die Mobilfunkanbieter-Apps In-App-Käufe für Nutzer:innen unterstützen. Derartige Abonnements dürfen keinen Zugriff auf oder Rabatte auf Verbrauchsartikel beinhalten und die Abonnements müssen zeitgleich mit dem Mobildatenvertrag enden.

3.1.2(b) Upgrades und Downgrades:

Nutzer:innen sollten ein nahtloses Upgrade-/Downgrade-Erlebnis haben und nicht in der Lage sein, versehentlich mehrere Variationen derselben Sache zu abonnieren. Lesen Sie die bewährten Vorgehensweisen zur Verwaltung der Upgrade- und Downgrade-Optionen für Ihr Abonnement.

3.1.2(c) Abonnementinformationen

Bevor Sie Kund:innen zum Abschließen eines Abonnements auffordern, müssen Sie klar beschreiben, welche Leistungen die Nutzer:innen für den Preis erhalten. Wie viele Ausgaben pro Monat? Wie viel Cloudspeicher? Welche Art von Zugriff auf Ihren Service? Stellen Sie sicher, dass Sie die in Anhang 2 der Lizenzvereinbarung für das Apple Developer Program aufgeführten Anforderungen klar kommunizieren.

3.1.3 Weitere Kaufmethoden

Bei den folgenden Apps werden möglicherweise andere Kaufmethoden als In-App-Käufe verwendet. Die Apps in diesem Abschnitt dürfen Nutzer:innen innerhalb der App nicht dazu ermutigen, eine andere Kaufmethode als den In-App-Kauf zu verwenden, mit Ausnahme der Bestimmungen in 3.1.3(a). Entwickler:innen dürfen außerhalb der App Mitteilungen über andere Kaufmethoden als In-App-Käufe an ihre Nutzerbasis senden.

3.1.3(a) „Reader"-Apps

Apps dürfen es Nutzer:innen ermöglichen, auf zuvor gekaufte Inhalte oder Inhaltsabonnements zuzugreifen (insbesondere: Zeitschriften, Zeitungen, Bücher, Audio, Musik und Videos). Reader-Apps dürfen die Erstellung von Accounts für kostenlose Stufen und die Accountverwaltung für bestehende Kund:innen anbieten. Entwickler:innen von Reader-Apps dürfen die Accountberechtigung für externe Links beantragen, um in ihrer App einen informativen Link zu einer Website bereitzustellen, die sich im Eigentum oder in der Verantwortung des:der Entwickler:in befindet, um einen Account zu erstellen oder zu verwalten. Erfahren Sie mehr über die Accountberechtigung für externe Links.

3.1.3(b) Plattformübergreifende Dienste

Apps, die plattformübergreifend verwendet werden, dürfen Nutzer:innen den Zugriff auf Inhalte, Abonnements oder Features ermöglichen, die sie in Ihrer App auf anderen Plattformen oder auf Ihrer Website erworben haben, einschließlich Verbrauchsgütern in plattformübergreifenden Spielen, sofern diese Elemente auch als In-App-Käufe in der App verfügbar sind.

3.1.3(c) Unternehmensdienste

Wenn Ihre App nur direkt von Ihnen an Organisationen oder Gruppen für deren Mitarbeiter:innen oder Schüler:innen verkauft wird (beispielsweise professionelle Datenbanken und Tools zur Klassenzimmerverwaltung), können Sie Unternehmensnutzer:innen den Zugriff auf zuvor gekaufte Inhalte oder Abonnements erlauben. Für Verkäufe an Endverbraucher:innen, Einzelnutzer:innen oder Familienmitglieder müssen In-App-Käufe verwendet werden.

3.1.3(d) Persönliche Dienste

Wenn Ihre App den Kauf von persönlichen Diensten in Echtzeit zwischen zwei Einzelpersonen ermöglicht (beispielsweise Nachhilfe für Student:innen, medizinische Konsultationen, Immobilienbesichtigungen oder Fitnesstrainings), können Sie andere Kaufmethoden als den In-App-Kauf für diese Zahlungen verwenden. Echtzeit-Dienste zwischen einer und mehreren oder einer und vielen Personen müssen per In-App-Kauf abgewickelt werden.

3.1.3(e) Waren und Dienste außerhalb der App

Wenn Ihre App den Kauf physischer Waren oder Dienste ermöglicht, die außerhalb der App verwendet werden, müssen Sie für diese Zahlungen andere Kaufmethoden als In-App-Käufe verwenden, z. B. Apple Pay oder die herkömmliche Kreditkartenzahlung.

3.1.3(f) Kostenlose eigenständige Apps

Für kostenlose Apps, die als eigenständige Ergänzung eines kostenpflichtigen webbasierten Tools fungieren (z. B. VoIP, Cloudspeicher, E-Mail-Dienste, Webhosting), müssen keine In-App-Käufe verwendet werden, sofern innerhalb der App kein Kauf bzw. keine Aufforderung zum Kauf außerhalb der App stattfindet.

3.1.3(g) Werbemanagement-Apps

Für Apps, die dem alleinigen Zweck dienen, Werbetreibenden (Personen oder Unternehmen, die für ein Produkt, einen Dienst oder ein Event werben) den Kauf und die Verwaltung von Werbekampagnen für alle Medientypen (Fernsehen, Außenwerbung, Websites, Apps usw.) zu ermöglichen, müssen keine In-App-Käufe verwendet werden. Diese Apps dienen der Kampagnenverwaltung und zeigen die Anzeigen selbst nicht an. Für digitale Käufe von Inhalten, die in einer App aufgerufen oder verwendet werden, einschließlich des Kaufs von Anzeigen, die in derselben App angezeigt werden (z. B. Verkäufe von „Boosts“ für Posts in einer Social-Media-App), müssen In-App-Käufe verwendet werden.

3.1.4 Hardwarespezifische Inhalte

Unter bestimmten Umständen, z. B. wenn die Funktionalität von Features abhängig von einer spezifischen Hardware ist, darf diese Funktionalität in der App auch ohne In-App-Kauf freigeschaltet werden (z. B. eine Astronomie-App, die Features hinzufügt, wenn sie mit einem Teleskop synchronisiert wird). Bei App-Features, die in Kombination mit einem zugelassenen physischen Produkt (etwa einem Spielzeug) auf optionaler Basis verwendet werden, dürfen Funktionen ohne In-App-Käufe freigeschaltet werden, sofern eine In-App-Kaufoption ebenfalls verfügbar ist. Sie dürfen von Nutzer:innen jedoch nicht verlangen, verwandte Produkte zu kaufen oder an Werbe- oder Marketingaktivitäten teilzunehmen, um die App-Funktionalität freizuschalten.

3.1.5 Kryptowährungen

(i) Wallets: Apps dürfen die Speicherung von virtueller Währung ermöglichen, sofern sie von Entwickler:innen angeboten werden, die als Organisation registriert sind.

(ii) Mining: Apps dürfen kein Mining von Kryptowährungen durchführen, es sei denn, die Verarbeitung erfolgt außerhalb des Geräts (z. B. cloudbasiertes Mining).

(iii) Börsen: Apps dürfen Transaktionen oder Übertragungen von Kryptowährung an einer zugelassenen Börse ermöglichen, sofern sie ausschließlich in Ländern oder Regionen angeboten werden, in denen die App über die entsprechenden Lizenzen und Berechtigungen zum Bereitstellen einer Kryptowährungsbörse verfügt.

(iv) Initial Coin Offerings: Apps, die Initial Coin Offerings („ICOs“), den Handel mit Kryptowährungen und andere Geschäfte mit Kryptowährung oder wertpapierähnliche Geschäfte ermöglichen, müssen von etablierten Banken, Wertpapierfirmen, Futures Commission Merchants („FCM“) oder anderen zugelassenen Finanzinstituten stammen und alle geltenden Gesetze einhalten.

(v) Kryptowährungs-Apps dürfen keine Währung für das Ausführen von Aufgaben anbieten, z. B. das Laden anderer Apps, das Ermutigen anderer Nutzer:innen zum Laden oder das Posten in sozialen Netzwerken.

3.2 Andere Probleme mit dem Geschäftsmodell

Die folgenden Listen sind nicht vollständig und Ihre Einreichung zieht möglicherweise eine Änderung oder Aktualisierung unserer Richtlinien nach sich, aber hier finden Sie einige allgemeine Regeln:

3.2.1 Zulässig

(i) Das Anzeigen eigener Apps für den Kauf oder die Werbung in Ihrer App, sofern die App nicht nur ein Katalog Ihrer Apps ist.

(ii) Das Anzeigen oder Empfehlen einer Sammlung von Apps von Dritten, die für einen bestimmten zugelassenen Zweck entwickelt wurden (z. B. Gesundheitsmanagement, Luftfahrt, Barrierefreiheit). Ihre App sollte umfassende redaktionelle Inhalte bereitstellen, damit sie nicht nur wie eine Store-Seite wirkt.

(iii) Die Deaktivierung des Zugriffs auf bestimmte zugelassene Leihinhalte (z. B. Filme, Fernsehprogramme, Musik, Bücher) nach Ablauf der Leihdauer; alle anderen Artikel und Dienste dürfen nicht ablaufen.

(iv) Wallet-Karten dürfen verwendet werden, um Zahlungen zu tätigen oder zu empfangen, Angebote zu übermitteln oder sich zu identifizieren (z. B. Kinokarten, Coupons und VIP-Anmeldedaten). Die anderweitige Verwendung führt möglicherweise zur Ablehnung der App und zum Entzug der Wallet-Anmeldedaten.

(v) Versicherungs-Apps müssen kostenlos sein, den gesetzlichen Bestimmungen der Regionen, in denen sie verteilt werden, entsprechen und dürfen keine In-App-Käufe verwenden.

(vi) Zugelassene gemeinnützige Organisationen dürfen Spendenaktionen direkt in ihren eigenen Apps oder Apps von Dritten durchführen, sofern diese Spendenkampagnen alle App Review Richtlinien erfüllen und Apple Pay unterstützen. Diese Apps müssen offenlegen, wie die Mittel verwendet werden, alle geltenden Gesetze auf Bundes- und Landesebene einhalten und sicherstellen, dass angemessene Steuerquittungen für Spender verfügbar sind. Zusätzliche Informationen müssen App Review auf Anfrage zur Verfügung gestellt werden. Gemeinnützige Plattformen, die Spender mit anderen gemeinnützigen Organisationen vernetzen, müssen sicherstellen, dass alle in der App aufgeführten gemeinnützigen Organisationen den Zulassungsprozess für gemeinnützige Organisationen durchlaufen haben. Erfahren Sie, wie Sie eine zugelassene gemeinnützige Organisation werden.

(vii) Apps dürfen es einzelnen Nutzer:innen ermöglichen, einer anderen Person ohne In-App-Käufe ein Geldgeschenk zu geben, vorausgesetzt, (a) das Geschenk ist eine völlig freiwillige Wahl des Gebers und (b) 100 % der Mittel gehen an den:die Empfänger:in des Geschenks. Allerdings müssen für Geschenke, die zu irgendeinem Zeitpunkt im Zusammenhang mit dem Erhalt digitaler Inhalte oder Dienste stehen, In-App-Käufe verwendet werden.

(viii) Apps, die für den Finanzhandel, Investitionen oder zur Geldverwaltung verwendet werden, müssen von dem Finanzinstitut eingereicht werden, das diese Dienste ausführt.

3.2.2 Nicht zulässig

(i) Die Erstellung einer Benutzeroberfläche für die Anzeige von Apps, Erweiterungen oder Plug-ins von Dritten, die dem App Store ähnelt, oder für eine Sammlung allgemeiner Art ist nicht zulässig.

(ii) Absichtlich ausgelassen.

(iii) Die künstliche Erhöhung der Anzahl der Impressions oder Click-Throughs von Anzeigen sowie von Apps, die hauptsächlich zur Ansicht von Anzeigen entwickelt wurden.

(iv) Das Sammeln von Geldern für Wohltätigkeitsorganisationen und Spendenaktionen innerhalb der App, es sei denn, Sie sind eine zugelassene gemeinnützige Organisation oder dies ist anderweitig gemäß Abschnitt 3.2.1 (vi) zulässig. Apps, mit denen für derartige Zwecke Gelder gesammelt werden sollen, müssen im App Store kostenlos sein und dürfen nur außerhalb der App, z. B. über Safari oder SMS, Gelder sammeln.

(v) Die willkürliche Einschränkung dessen, wer die App nutzen darf, z. B. nach Standort oder Mobilfunkanbieter.

(vi) Absichtlich ausgelassen.

(vii) Die künstliche Manipulation der Sichtbarkeit, des Status oder des Rangs von Nutzer:innen in anderen Diensten, es sei denn, dies ist gemäß den allgemeinen Geschäftsbedingungen dieses Dienst zulässig.

(viii) Apps, die den Handel mit binären Optionen ermöglichen, sind im App Store nicht erlaubt. Ziehen Sie stattdessen eines Web-App in Betracht. Apps, die den Handel mit Differenzkontrakten (Contracts for Difference, „CFDs“) oder anderen Derivaten (z. B. FOREX) ermöglichen, müssen in allen Ländern, in denen der Service verfügbar ist, ordnungsgemäß lizenziert werden.

(ix) Apps, die Privatkredite anbieten, müssen sämtliche Kreditbedingungen klar und deutlich offenlegen, einschließlich, aber nicht beschränkt auf den entsprechenden maximalen effektiver Jahreszins (Annual Percentage Rate, APR) und das Fälligkeitsdatum der Zahlung. Apps dürfen keinen maximalen APR von mehr als 36 % einschließlich Kosten und Gebühren erheben und keine vollständige Rückzahlung in 60 Tagen oder weniger verlangen.

4. Design

Apple Kund:innen legen großen Wert auf Produkte, die einfach, hochwertig, innovativ und benutzerfreundlich sind, und genau das möchten wir auch im App Store sehen. Es liegt an Ihnen, ein tolles Design zu erstellen, doch die folgenden Mindeststandards müssen Sie in jedem Fall einhalten, um eine Genehmigung für den App Store zu erhalten. Denken Sie daran, dass Sie Ihre App auch nach der Genehmigung aktualisieren müssen, um sicherzustellen, dass sie weiterhin funktioniert und sowohl neue als auch bestehende Kund:innen anspricht. Apps, die nicht mehr funktionieren oder nur ein eingeschränktes Erlebnis bieten, können jederzeit aus dem App Store entfernt werden.

4.1 Nachahmer

(a) Lassen Sie sich Ihre eigenen Ideen einfallen. Wir wissen, dass Sie sie haben, doch Sie müssen sie auch in die Praxis umsetzen. Sie dürfen nicht einfach die aktuellste beliebte App im App Store kopieren oder einige kleinere Änderungen am Namen oder der Benutzeroberfläche einer anderen App vornehmen und diese als Ihre eigene ausgeben. Zusätzlich zum Risiko einer Klage wegen Verletzung des geistigen Eigentums erschwert das die Navigation im App Store und ist gegenüber anderen Entwickler:innen einfach nicht fair.

(b) Das Einreichen von Apps, die andere Apps oder Dienste imitieren, gilt als Verstoß gegen den Verhaltenskodex für Entwickler:innen und kann zum Ausschluss aus dem Apple Developer Program führen.

4.2 Mindestfunktionalität

Ihre App muss Features, Inhalte und eine Benutzeroberfläche umfassen, die sie von einer neu aufbereiteten Website abhebt. Apps, die nicht besonders nützlich oder nicht einzigartig sind bzw. sich nicht wie eine typische App verhalten, sind im App Store fehl am Platz. Wenn Ihre App keinen dauerhaften Unterhaltungswert oder angemessenes Nutzen bietet, wird sie unter Umständen nicht akzeptiert. Apps, bei denen es sich lediglich um einen Song oder Film handelt, müssen beim iTunes Store eingereicht werden. Apps, bei denen es sich lediglich um ein Buch oder Spielehandbuch handelt, müssen beim Apple Books Store eingereicht werden.

4.2.1 Apps, die ARKit verwenden, müssen umfassende und integrierte Augmented-Reality-Erlebnisse bieten. Es reicht nicht aus, nur ein Modell in einer AR-Ansicht darzustellen oder eine Animation abzuspielen.

4.2.2 Abgesehen von Katalogen darf es sich bei Apps nicht in erster Linie um Marketingmaterialien, Anzeigen, Web-Clippings, eine Zusammenstellung von Inhalten oder eine Sammlung von Links handeln.

4.2.3

(i) Ihre App muss eigenständig funktionieren, ohne dass dafür eine andere App installiert werden muss.

(ii) Wenn Ihre App zusätzliche Ressourcen laden muss, um beim ersten Start zu funktionieren, geben Sie die Größe des Downloads an und informieren Sie die Nutzer:innen im Voraus.

4.2.4 Absichtlich ausgelassen.

4.2.5 Absichtlich ausgelassen.

4.2.6 Apps, die über eine kommerzielle Vorlage oder einen App-Generierungsdienst erstellt wurden, werden abgelehnt, es sei denn, sie werden direkt vom Anbieter der App-Inhalte eingereicht. Diese Dienste dürfen keine Apps im Namen ihrer Kund:innen einreichen und müssen Tools anbieten, mit denen ihre Kund:innen maßgeschneiderte, innovative Apps erstellen können, die einzigartige Kundenerlebnisse bieten. Eine weitere zulässige Option für Vorlagenanbieter besteht darin, eine einzige Binärdatei zu erstellen, um alle Kundeninhalte in einem aggregierten oder einem „Auswahlmodell" zu hosten, z. B. als App zum Finden von Restaurants mit separaten benutzerdefinierten Einträgen oder Seiten für jedes Kundenrestaurant oder als Ereignis-App mit separaten Einträge für jedes Kundenereignis.

4.2.7 Remote Desktop Clients

Wenn Ihre Remote Desktop-App als Spiegel spezifischer Software oder Dienste statt als generischer Spiegel des Hostgeräts fungiert, muss sie Folgendes erfüllen:

(a) Die App darf sich nur mit einem Hostgerät im Besitz der Nutzer:innen verbinden, bei dem es sich um einen PC oder eine dedizierte Spielkonsole der Nutzer:innen handelt, und sowohl das Hostgerät als auch der Client müssen über ein lokales und LAN-basiertes Netzwerk verbunden sein.

(b) Jegliche Software oder Dienste im Client werden vollständig auf dem Hostgerät ausgeführt (wiedergegeben auf dem Bildschirm des Hostgeräts) und dürfen keine APIs oder Plattformfeatures verwenden, die über die zum Streamen des Remote Desktop erforderlichen hinausgehen.

(c) Die Erstellung und Verwaltung von Accounts muss vom Hostgerät aus gestartet werden.

(d) Die auf dem Client angezeigte Benutzeroberfläche darf keiner iOS oder App Store Ansicht ähneln, keine Store-ähnliche Oberfläche bereitstellen und nicht die Möglichkeit bieten, Software zu durchsuchen, auszuwählen oder zu kaufen, die nicht bereits im Besitz der Nutzer:innen ist oder von diesen lizenziert wurde. Aus Gründen der Genauigkeit müssen bei Transaktionen, die in gespiegelter Software stattfinden, keine In-App-Käufe verwendet werden, sofern die Transaktionen auf dem Hostgerät verarbeitet werden.

(e) Thin Clients für cloudbasierte Apps sind für den App Store nicht geeignet.

4.3 Spam

(a) Erstellen Sie nicht mehrere Paket-IDs derselben App. Wenn Ihre App verschiedene Versionen für bestimmte Standorte, Sportmannschaften, Universitäten usw. umfasst, können Sie auch eine einzelne App einreichen und die Variationen im Rahmen von In-App-Käufen bereitstellen.

(b) Vermeiden Sie außerdem bereits übersättigte Kategorien. Der App Store enthält bereits genügend Apps in Sachen Furzen, Rülpsen, Taschenlampen, Wahrsagerei, Dating, Trinkspiele, Kama Sutra. usw. Wir werden diese Apps ablehnen, sofern sie kein einzigartiges, qualitativ hochwertiges Erlebnis bieten. Spam im Store kann dazu führen, dass Sie aus dem Apple Developer Program entfernt werden.

4.4 Erweiterungen

Apps, die Erweiterungen hosten oder enthalten, müssen die Bestimmungen des App Extension Programming Guide (Programmierhandbuch für App-Erweiterungen), des Safari App Extensions Guide (Handbuch für Safari-App-Erweiterungen) oder der Safari Web Extensions Documentation (Dokumentation zu Safari-Web-Erweiterungen) erfüllen und sollten, wenn möglich, zumindest einige Funktionen wie Hilfebildschirme und bestimmte Einstellungsfenster bieten. Sie müssen klar und deutlich angeben, welche Erweiterungen im Marketingtext der App verfügbar sein werden, und die Erweiterungen dürfen kein Marketing, keine Werbung und keine In-App-Käufe enthalten.

4.4.1 Für Tastaturerweiterungen gelten einige zusätzliche Regeln.

Diese müssen:

- Funktionen für die Tastatureingabe bereitstellen (z. B. eingegebene Zeichen);
- Die Sticker-Richtlinien einhalten, wenn die Tastatur Bilder oder Emojis enthält;
- Eine Methode bereitstellen, um zur nächsten Tastatur zu gelangen;
- Auch ohne Netzwerkzugriff und ohne die Anforderung des vollständigen Zugriffs funktionstüchtig sein;
- Erfassen Sie Nutzeraktivitäten nur, um die Funktionalität der Tastaturerweiterung der Nutzer:innen auf dem iOS Gerät zu verbessern.

Folgendes ist nicht zulässig:

- Neben den Einstellungen weitere Apps starten; oder
- Tastaturtasten für andere Verhaltensweisen verwenden (z. B. Gedrückthalten des „Zeilenschalters“ zum Starten der Kamera).

4.4.2 Safari-Erweiterungen müssen mit der aktuellen Version von Safari auf dem entsprechenden Apple Betriebssystem laufen. Sie dürfen keine Elemente des Systems oder der Safari Benutzeroberfläche beeinträchtigen und dürfen niemals schädliche oder irreführende Inhalte oder Codes enthalten. Ein Verstoß gegen diese Bestimmung führt zur Entfernung aus dem Apple Developer Program. Safari-Erweiterungen dürfen keinen Zugriff auf mehr Websites beanspruchen, als für die Funktionsweise unbedingt erforderlich sind.

4.4.3 Absichtlich ausgelassen.

4.5 Apple Websites und Dienste

4.5.1 Apps dürfen zugelassene Apple RSS Feeds wie den iTunes Store RSS Feed verwenden, aber keine Informationen von Apple Websites (z. B. apple.com, iTunes Store, App Store, App Store Connect, Developer Portal) auslesen oder mithilfe dieser Informationen Rankings erstellen.

4.5.2 Apple Music

(i) Mit MusicKit unter iOS können Nutzer:innen Apple Music und ihre lokale Musikbibliothek nativ von Ihren Apps und Spielen aus abspielen. Wenn ein:e Nutzer:in dem Apple Music Account die Berechtigung erteilt, kann Ihre App Playlists erstellen, Songs zu Playlist hinzufügen und einen der Millionen von Songs im Apple Music Katalog abspielen. Nutzer:innen müssen die Wiedergabe eines Apple Music Streams starten und in der Lage sein, mithilfe der standardmäßigen Mediensteuerelemente wie „Wiedergabe", „Pause" und „Überspringen" zu navigieren. Darüber hinaus darf Ihre App keine Zahlung verlangen oder den Zugriff auf den Apple Music Service indirekt monetarisieren (z. B. durch In-App-Käufe, Werbung, Anfordern von Nutzerinformationen). Sie dürfen keine Musikdateien aus den MusicKit APIs herunter- oder hochladen oder deren Freigabe ermöglichen, es sei denn, dies ist ausdrücklich gemäß der Dokumentation zu MusicKit zulässig.

(ii) Die Verwendung der MusicKit APIs ist kein Ersatz für das Einholen der Lizenzen, die Sie für eine umfassendere oder komplexere Musikintegration möglicherweise benötigen. Wenn Sie beispielsweise möchten, dass Ihre App einen bestimmten Song zu einem bestimmten Zeitpunkt wiedergibt oder Audio- oder Videodateien erstellt, die in sozialen Medien geteilt werden können, müssen Sie sich direkt an die Rechteinhaber wenden, um deren Genehmigung (z. B. das Recht zur Synchronisierung oder Anpassung) und Assets einzuholen. Coverbilder und andere Metadaten dürfen nur im Zusammenhang mit der Musikwiedergabe oder Playlists (einschließlich Bildschirmfotos aus dem, die die Funktionalität Ihrer App zeigen) verwendet werden und dürfen nicht für Marketing- oder Werbezwecke verwendet werden, ohne die ausdrückliche Genehmigung der Rechteinhaber einzuholen. Befolgen Sie die Apple Music Identity Guidelines (Identitätsrichtlinien für Apple Music) beim Einbinden von Apple Music Diensten in Ihre App.

(iii) Apps, die auf Apple Music Nutzerdaten zugreifen, z. B. Playlists und Favoriten, müssen diesen Zugriff eindeutig im Purpose String angeben. Die gesammelten Daten dürfen nicht zu anderen Zwecken als zur Unterstützung oder Verbesserung des App-Erlebnisses an Dritte weitergegeben werden. Diese Daten dürfen nicht verwendet werden, um Nutzer:innen oder Geräte zu identifizieren oder Werbung zu machen.

4.5.3 Verwenden Sie Apple Dienste nicht für Spam, Phishing und auch nicht, um unaufgefordert Nachrichten an Kund:innen zu senden. Dies schließt Game Center, Push-Mitteilungen usw. ein. Versuchen Sie nicht, Spieler-IDs, Aliasse oder andere über das Game Center erhaltene Informationen zurückzuverfolgen, nachzuverfolgen, zu verknüpfen, zuzuordnen, zu minen, zu sammeln oder anderweitig verwenden, sonst werden Sie aus dem Apple Developer Program entfernt.

4.5.4 Push-Mitteilungen dürfen für die Funktion der App nicht erforderlich sein und nicht zum Senden sensibler personenbezogener oder vertraulicher Daten verwendet werden. Push-Mitteilungen sollten nicht für Werbe- oder Direktmarketingzwecke verwendet werden, es sei denn, Kund:innen haben sich ausdrücklich dafür entschieden, sie über die in der Benutzeroberfläche Ihrer App angezeigte Zustimmungssprache zu erhalten, und Sie stellen in Ihrer App eine Methode bereit, mit der ein:e Nutzer:in solche Nachrichten abbestellen kann. Der Missbrauch dieser Dienste kann zum Widerruf Ihrer Berechtigungen führen.

4.5.5 Verwenden Sie Game Center Spieler-IDs nur in einer Weise, die gemäß den Bedingungen für das Game Center zulässig ist, und zeigen Sie sie nicht in der App oder für Dritte an.

4.5.6 Apps dürfen Unicode-Zeichen verwenden, die in der App und den App-Metadaten als Apple Emojis dargestellt werden. Apple Emojis dürfen nicht auf anderen Plattformen verwendet oder direkt in Ihre App-Binärdatei eingebettet werden.

4.6 Alternative App-Symbole

Apps dürfen benutzerdefinierte Symbole anzeigen, um z. B. eine Vorliebe für eine bestimmte Sportmannschaft auszudrücken, vorausgesetzt, dass jede Änderung von Nutzer:innen initiiert wird und die App Einstellungen zum Zurücksetzen auf das ursprüngliche Symbol umfasst. Alle Symbolvarianten müssen sich auf den Inhalt der App beziehen und die Änderungen sollten über alle Systemassets hinweg einheitlich sein, sodass die in den Einstellungen, Mitteilungen usw. angezeigten Symbole mit dem neuen Springboard-Symbol übereinstimmen.

4.7 Mini-Apps, Mini-Spiele, Streamingspiele, Chatbots, Plug-ins und Spiel-Emulatoren

Von Apps kann bestimmte Software angeboten werden, die nicht in die Binärdatei eingebettet ist, insbesondere HTML5-Mini-Apps und -Mini-Spiele, Streamingspiele, Chatbots, und Plug-ins. Darüber hinaus können Emulator-Apps für Retro-Spielekonsolen den Download von Spielen anbieten. Sie sind für die gesamte in Ihrer App angebotene Software verantwortlich, einschließlich der Sicherstellung, dass diese Software diesen Richtlinien und allen geltenden Gesetzen entspricht. Software, die einen oder mehreren Richtlinien nicht entspricht, führt zur Ablehnung Ihrer App. Außerdem müssen Sie sicherstellen, dass die Software den zusätzlichen Regeln in 4.7.1 und 4.7.5 entspricht. Diese zusätzlichen Regeln sind wichtig, um das Erlebnis aufrechtzuerhalten, das Kund:innen im App Store erwarten, und um die Sicherheit der Nutzer:innen zu gewährleisten.

4.7.1 Auf Software, die gemäß dieser Regel in Apps angeboten wird, muss Folgendes zutreffen:

- Sie muss allen Datenschutzrichtlinien entsprechen, einschließlich, aber nicht beschränkt auf die Regeln in Richtlinie 5.1 zur Erfassung, Nutzung und Freigabe von Daten und sensiblen Daten (z. B. Gesundheits- und personenbezogene Daten von Kindern);
- Sie muss eine Methode zum Filtern von anstößigen Materialien, einen Mechanismus zum Melden von Inhalten und zeitnahen Reaktionen auf Bedenken sowie die Möglichkeit, missbräuchliche Nutzer:innen zu blockieren, umfassen; und
- Sie muss In-App-Käufe verwenden, um Endnutzer:innen digitale Waren oder Dienste anzubieten.

4.7.2 Ihre App darf ohne vorherige Zustimmung von Apple keine nativen Plattform-APIs auf die Software ausweiten oder dieser zur Verfügung stellen.

4.7.3 Ihre App darf ohne ausdrückliche Zustimmung der Nutzer:innen in der jeweiligen Instanz keine Daten oder Datenschutzberechtigungen für einzelne in Ihrer App angebotene Software teilen.

4.7.4 Sie müssen einen Index der in Ihrer App verfügbaren Software und Metadaten bereitstellen. Dieser muss universelle Links enthalten, die zu der gesamten in Ihrer App angebotenen Software führen.

4.7.5 Ihre App muss die Altersfreigabe der Inhalte mit der höchsten Altersfreigabe, die in Ihrer App verfügbar sind, angeben.

4.8 Anmeldedienste

Apps, die einen Anmeldedienst eines Dritten verwenden oder sich über die sozialen Medien anmelden (z. B. Facebook Login, Google Sign-In, Sign in with Twitter, Sign In with LinkedIn, Login with Amazon oder WeChat Login), um den primären Account des:der Nutzer:in über die App einzurichten oder zu authentifizieren, müssen außerdem als gleichwertige Option einen weiteren Anmeldedienst mit den folgenden Features anbieten:

- Der Anmeldedienst beschränkt die Datenerfassung auf den Namen und die E-Mail-Adresse des:der Nutzer:in;
- Mit dem Anmeldedienst können Nutzer:innen ihre E-Mail-Adresse bei der Einrichtung ihres Accounts privat halten; und
- Der Anmeldedienst erfasst ohne Zustimmung keine Interaktionen mit Ihrer App zu Werbezwecken.

Der primäre Account ist der Account, den Nutzer:innen mit Ihrer App für Identifizierung, Anmeldung und Zugriff auf Features und verknüpfte Dienste einrichten.

In folgenden Fällen ist kein weiterer Anmeldedienst erforderlich:

- Ihre App verwendet ausschließlich die eigenen Systeme Ihres Unternehmens für die Einrichtung und Anmeldung.

- Ihre App ist ein alternativer App-Marktplatz oder eine App, die über einen alternativen App-Marktplatz verteilt wird und eine marktplatzspezifische Anmeldung für Account-, Download- und Commerce-Funktionen verwendet.

- Bei Ihrer App handelt es sich um eine App für Bildungseinrichtungen, Unternehmen oder Geschäftsbereiche, bei der sich die Nutzer:innen mit einem bestehenden Account für Bildungseinrichtungen oder Unternehmen anmelden muss.

- Ihre App verwendet ein von der Regierung oder der Industrie unterstütztes Bürgeridentifizierungssystem oder eine elektronische ID, um Nutzer:innen zu authentifizieren.

- Ihre App ist ein Client für einen bestimmten Service von Dritten und die Nutzer:innen müssen sich direkt bei ihrem E-Mail-, Social-Media- oder anderen Account des Dritten anmelden, um auf ihre Inhalte zuzugreifen.

4.9 Apple Pay

Apps, die Apple Pay verwenden, müssen den Nutzer:innen vor dem Kauf sämtlicher Waren und Dienste alle wesentlichen Kaufinformationen zur Verfügung stellen und die Apple Pay Marketing Guidelines (Marketingrichtlinien für Apple Pay) und die Human Interface Guidelines (Richtlinien für Nutzerschnittstellen) wie beschrieben verwenden. Apps, die für wiederkehrende Zahlungen Apple Pay verwenden, müssen mindestens die folgenden Informationen offenlegen:

- Die Dauer des Verlängerungszeitraums und die Tatsache, dass dieser bis zur Kündigung läuft
- Was im jeweiligen Zeitraum bereitgestellt wird
- Die tatsächlichen Kosten, die Kund:innen in Rechnung gestellt werden
- Wie die Kündigung funktioniert

4.10 Monetarisierung integrierter Funktionen

Sie dürfen die von der Hardware oder dem Betriebssystem bereitgestellten integrierten Funktionen, wie Push-Mitteilungen, die Kamera oder das Gyroskop, oder Apple Dienste und Technologien, wie den Zugriff auf Apple Music, iCloud Speicher oder Bildschirmzeit-APIs, nicht monetarisieren.

---

5. Rechtliche Hinweise

Apps müssen den rechtlichen Bestimmungen aller Standorte entsprechen, an denen Sie sie zur Verfügung stellen (wenden Sie sich an einen Anwalt, wenn Sie sich nicht sicher sind). Diese Dinge sind zwar kompliziert, doch es liegt in Ihrer Verantwortung, die lokalen Gesetze nachzuvollziehen und sicherzustellen, dass Ihre App diesen entspricht, nicht nur den nachfolgenden Richtlinien. Natürlich werden Apps abgelehnt, die zu kriminellem oder eindeutig leichtsinnigem Verhalten auffordern, dieses fördern oder bewerben. In Extremfällen, z. B. bei Apps, die Menschenhandel und/oder die Ausbeutung von Kindern fördern, werden die zuständigen Behörden informiert.

5.1 Datenschutz

Der Datenschutz der Nutzer:innen ist im Apple Ökosystem von größter Bedeutung und Sie müssen sorgfältig mit personenbezogenen Daten umgehen, um sicherzustellen, dass Sie die bewährten Vorgehensweisen für den Datenschutz, die geltenden Gesetze und die Bestimmungen der Lizenzvereinbarung für das Apple Developer Program einhalten, ganz zu schweigen von den Erwartungen der Kund:innen. Insbesondere gilt Folgendes:

5.1.1 Datenerfassung und -speicherung

(i) Datenschutzrichtlinien: Alle Apps müssen im Metadatenfeld in App Store Connect und innerhalb der App einen leicht zugänglichen Link zur Datenschutzrichtlinie enthalten. Die Datenschutzrichtlinie muss Folgendes klar und deutlich darlegen:

- Welche Daten gegebenenfalls von der App/dem Service erfasst werden, wie diese Daten erfasst werden und wie sie genutzt werden.

- Die Tatsache, dass alle Dritten, mit denen eine App Nutzerdaten teilt (in Übereinstimmung mit diesen Richtlinien) – z. B. Analysetools, Werbenetzwerke und SDKs von Dritten sowie alle Mutter- und Tochterunternehmen und anderen verbundenen Unternehmen, die Zugriff auf die Nutzerdaten haben – Nutzerdaten in gleichem oder vergleichbarem Maß schützen wie in der Datenschutzrichtlinie der App angegeben und durch diese Richtlinien vorgeschrieben.

- Die Richtlinien zur Aufbewahrung/Löschung von Daten und die Vorgehensweise, wenn Nutzer:innen die Einwilligung widerrufen und/oder die Löschung der Nutzerdaten anfordern möchten.

(ii) Zustimmung: Apps, die Nutzer- oder Nutzungsdaten erfassen, müssen die Zustimmung der Nutzer:innen für die Erfassung einholen, auch wenn diese Daten zum Zeitpunkt der Erfassung oder unmittelbar nach der Erfassung anonymisiert werden. Kostenpflichtige Funktionen dürfen nicht von einem:einer Nutzer:in abhängig sein oder davon abhängen, dass der:die Nutzer:in den Zugriff auf diese Daten gewährt. Apps müssen Kund:innen außerdem eine leicht zugängliche und verständliche Möglichkeit bieten, ihre Zustimmung zu widerrufen. Stellen Sie sicher, dass in Ihren Purpose Strings die Verwendung der Daten klar und vollständig beschrieben wird. Apps, die ohne Zustimmung Daten für ein berechtigtes Interesse erfassen, indem sie sich auf die Bestimmungen der Datenschutz-Grundverordnung („DSGVO“) der EU oder eines ähnlichen Gesetzes stützen, müssen alle Bestimmungen dieses Gesetzes einhalten. Erfahren Sie mehr über das Einholen der Zustimmung.

(iii) Datensparsamkeit: Apps dürfen nur Zugriff auf Daten anfordern, die im Zusammenhang mit der Kernfunktionalität der App stehen, und ausschließlich Daten erfassen und verwenden, die zur Erfüllung der jeweiligen Aufgabe erforderlich sind. Verwenden Sie nach Möglichkeit die prozessexterne Auswahl oder ein Freigabeformular, anstatt den vollen Zugriff auf geschützte Ressourcen wie Fotos oder Kontakte anzufordern.

(iv) Zugriff: Apps müssen die Berechtigungseinstellungen der Nutzer:innen einhalten und dürfen nicht versuchen, Personen zu manipulieren, auszutricksen oder dazu zu zwingen, einem unnötigen Datenzugriff zuzustimmen. Beispielsweise dürfen Apps, die Fotos in einem sozialen Netzwerk veröffentlichen können, keinen Mikrofonzugriff anfordern, bevor die Nutzer:innen Fotos hochladen können. Stellen Sie nach Möglichkeit alternative Lösungen für Nutzer:innen bereit, die keine Einwilligung erteilen. Wollen Nutzer:innen beispielsweise ihren Standort nicht teilen, bieten Sie die Option an, die Adresse manuell einzugeben.

(v) Accountanmeldung: Wenn Ihre App keine wichtigen accountbasierten Features enthält, sollten die Nutzer:innen sie ohne Anmeldung verwenden können. Wenn Ihre App die Erstellung eines Accounts unterstützt, müssen Sie auch das Löschen des Accounts in der App anbieten. Apps dürfen nicht verlangen, dass Nutzer:innen personenbezogene Daten eingeben, damit die App funktioniert,

es sei denn, diese Daten sind für die Kernfunktionalität der App unmittelbar relevant oder gesetzlich vorgeschrieben. Wenn die Kernfunktionalität Ihrer App nicht im Zusammenhang mit einem bestimmten sozialen Netzwerk steht (z. B. Facebook, WeChat, Weibo, X usw.), müssen Sie den Zugriff ohne Anmeldung oder über einen anderen Mechanismus bereitstellen. Das Abrufen grundlegender Profildaten, das Teilen in sozialen Netzwerken oder das Einladen von Freunden zur Nutzung der App zählen nicht zu den Kernfunktionen der App. Die App muss außerdem innerhalb der App einen Mechanismus zum Widerrufen der Anmeldedaten für soziale Netzwerke und zum Deaktivieren des Datenzugriffs zwischen der App und dem sozialen Netzwerk enthalten. Eine App darf keine Anmeldedaten oder Tokens für soziale Netzwerke außerhalb des Geräts sichern und darf derartige Anmeldedaten oder Tokens nur verwenden, um direkt in der App eine Verbindung zu dem sozialen Netzwerk herzustellen, während die App verwendet wird.

(vi) Entwickler:innen, die ihre Apps einsetzen, um Passwörter oder andere private Daten unauffällig abzufragen, werden aus dem Apple Developer Program entfernt.

(vii) SafariViewController muss verwendet werden, um Nutzer:innen Informationen sichtbar zu präsentieren; der Controller darf nicht durch andere Ansichten oder Ebenen verdeckt oder verborgen werden. Darüber hinaus darf eine App SafariViewController nicht verwenden, um Nutzer:innen ohne deren Wissen und Einwilligung nachzuverfolgen.

(viii) Apps, die personenbezogene Daten aus einer beliebigen Quelle zusammenstellen, die nicht direkt von Nutzer:innen stammt – einschließlich öffentlicher Datenbanken – oder dies ohne die ausdrückliche Einwilligung der Nutzer:innen tun, sind im App Store oder auf alternativen App-Marktplätzen nicht erlaubt.

(ix) Apps, die Dienste in stark regulierten Bereichen anbieten (z. B. Bank- und Finanzwesen, Gesundheitswesen, Glücksspiel, legaler Cannabiskonsum und Flugreisen) oder die vertrauliche Nutzerdaten erfordern, müssen von der juristischen Person eingereicht werden, die die Dienste bereitstellt, nicht von einem:einer einzelnen Entwickler:in. Apps, die den legalen Verkauf von Cannabis ermöglichen, müssen geografisch auf die entsprechende Gerichtsbarkeit beschränkt sein.

(x) Apps dürfen grundlegende Kontaktdaten (wie den Namen und die E-Mail-Adresse) abfragen, solange die Abfrage für die Nutzer:innen optional ist, die Features und Dienste nicht von der Bereitstellung der Daten abhängig sind und alle anderen Bestimmungen dieser Richtlinien eingehalten werden, einschließlich Einschränkungen zur Erfassung von Daten von Kindern.

5.1.2 Datennutzung und -freigabe

(i) Sofern nicht anderweitig gesetzlich zulässig, dürfen Sie keine personenbezogenen Daten verwenden, übermitteln oder teilen, ohne zuvor die Einwilligung der Person einzuholen. Sie müssen Informationen darüber zur Verfügung stellen, wie und wo die Daten verwendet werden. Aus Apps erfasste Daten dürfen nur an Dritte weitergegeben werden, um die App zu verbessern oder Werbung bereitzustellen (in Übereinstimmung mit der Lizenzvereinbarung für das Apple Developer Program). Sie müssen die ausdrückliche Erlaubnis von Nutzer:innen über die App Tracking Transparency APIs einholen, um ihre Aktivitäten nachzuverfolgen. Erfahren Sie mehr über die Nachverfolgung. Ihre App darf von den Nutzer:innen nicht verlangen, dass sie Systemfunktionen aktivieren (z. B. Push-

Mitteilungen, Ortungsdienste, Nachverfolgung), um auf Funktionen und Inhalte zuzugreifen, die App zu verwenden oder Geld oder andere Vergütungen zu erhalten, einschließlich, aber nicht beschränkt auf Geschenkkarten und Codes. Apps, die Nutzerdaten ohne Einwilligung der Nutzer:innen oder anderweitige Einhaltung von Datenschutzgesetzen teilen, werden möglicherweise aus dem Verkauf genommen und Sie werden unter Umständen aus dem Apple Developer Program entfernt.

(ii) Daten, die für einen bestimmten Zweck erfasst wurden, dürfen nicht ohne weitere Zustimmung weiterverwendet werden, sofern nicht gesetzlich ausdrücklich etwas anderes zulässig ist.

(iii) Apps dürfen nicht versuchen, auf der Grundlage erfasster Daten unauffällig ein Nutzerprofil zu erstellen, und dürfen nicht versuchen oder es anderen ermöglichen, anonyme Nutzer:innen zu identifizieren oder Nutzerprofile auf der Grundlage von Daten zu rekonstruieren, die von den von Apple bereitgestellten APIs oder Ihrer Aussage nach „anonymisiert", „aggregiert" oder auf andere nicht identifizierbare Weise erfasst wurden.

(iv) Verwenden Sie keine Informationen aus Kontakten, Fotos oder anderen APIs, die auf Nutzerdaten zugreifen, um eine Kontaktdatenbank für Ihre eigene Verwendung oder für den Verkauf/die Verteilung an Dritte zu erstellen, und erfassen Sie keine Informationen darüber, welche anderen Apps zu Analyse- oder Werbe-/Marketingzwecken auf dem Gerät eines:einer Nutzer:in installiert sind.

(v) Kontaktieren Sie keine Personen über die Informationen, die über die Kontakte oder Fotos eines:einer Nutzer:in erfasst wurden, es sei denn, ein:e einzelne:r Nutzer:in fordert Sie ausdrücklich dazu auf; integrieren Sie nicht die Option „Alle auswählen" oder die standardmäßige Auswahl aller Kontakte. Sie müssen für die Nutzer:innen vor dem Senden klar darlegen, wie ihre Nachricht für den:die Empfänger:in angezeigt wird (z. B.: Was wird in der Nachricht stehen? Wer wird als Absender angezeigt?).

(vi) Daten, die Sie aus der HomeKit-API, HealthKit, der Clinical Health Records-API, den MovementDisorder-APIs, ClassKit oder aus Tools für die Tiefen-/Gesichtserkennung (wie ARKit, Kamera-APIs oder Foto-APIs) gesammelt haben, dürfen nicht für Marketing, Werbung oder nutzerbezogene Datengewinnung, auch nicht durch Dritte, verwendet werden. Erfahren Sie mehr über die bewährten Vorgehensweisen für die Implementierung von CallKit, HealthKit, ClassKit, und ARKit.

(vii) Apps, die Apple Pay verwenden, dürfen über Apple Pay erfasste Nutzerdaten nur mit Dritten teilen, um die Bereitstellung von Waren und Diensten zu ermöglichen oder zu verbessern.

5.1.3 Gesundheit und Gesundheitsforschung

Gesundheits-, Fitness- und medizinische Daten sind besonders vertraulich und für Apps in diesem Bereich gelten einige zusätzliche Regeln, um sicherzustellen, dass die Privatsphäre der Kund:innen geschützt ist:

(i) Apps dürfen keine Daten, die im Zusammenhang mit Gesundheits-, Fitness- oder Gesundheitsforschung erfasst wurden, einschließlich mithilfe der Clinical Health Records-API, der HealthKit-API, von Bewegungs- und Fitnesssensoren, der MovementDisorder-APIs oder von gesundheitsbezogenen Studien mit Proband:innen erfassten Daten, zu Werbe- oder Marketingzwecken oder sonstiger nutzungsbasierter Datengewinnung verwenden oder an Dritte

weitergeben, es sei denn, dies dient der Verbesserung des Gesundheitsmanagements oder der Gesundheitsforschung und der:die Nutzer:in hat diesem zugestimmt. Apps dürfen jedoch die Gesundheits- oder Fitnessdaten von Nutzer:innen verwenden, um diesen unmittelbar einen Vorteil zu gewähren (z. B. eine günstigere Versicherungsprämie), vorausgesetzt, die App wird von der Stelle bereitgestellt, die den Vorteil anbietet, und die Daten werden nicht an Dritte weitergegeben. Sie müssen die spezifischen Gesundheitsdaten offenlegen, die Sie über das Gerät erfassen.

(ii) Apps dürfen keine falschen oder fehlerhaften Daten in HealthKit oder jegliche andere App für Gesundheitsmanagement oder -forschung schreiben und dürfen persönliche Gesundheitsdaten nicht in iCloud sichern.

(iii) Bei Apps, die gesundheitsbezogene klinische Studien durchführen, muss die Zustimmung der Teilnehmer oder bei Minderjährigen die Zustimmung der Eltern oder Erziehungsberechtigten eingeholt werden. Diese Zustimmung muss Folgendes umfassen: (a) Art, Zweck und Dauer der Forschung; (b) Verfahren, Risiken und Vorteile für den Teilnehmer; (c) Informationen zur Vertraulichkeit und zum Umgang mit Daten (einschließlich der Weitergabe an Dritte); (d) eine Anlaufstelle für Fragen der Teilnehmer; und (e) den Ablauf eines Widerrufs.

(iv) Apps, die gesundheitsbezogene klinische Studien durchführen, müssen von einer unabhängigen Ethikkommission genehmigt werden. Auf Anfrage muss ein entsprechender Nachweis vorgelegt werden.

5.1.4 Kinder

(a) Aus unterschiedlichen Gründen ist es enorm wichtig, sorgfältig mit personenbezogenen Daten von Kindern umzugehen, und wir empfehlen Ihnen, alle Anforderungen zur Einhaltung von Gesetzen wie dem „Gesetz zum Schutz der Privatsphäre von Kindern im Internet“ (Children’s Online Privacy Protection Act, „COPPA“), der Datenschutz-Grundverordnung der Europäischen Union („DSGVO“) und allen anderen geltenden Vorschriften oder Gesetzen sorgfältig durchzugehen.

Apps dürfen Geburtsdaten und Kontaktdaten der Eltern nur zum Zweck der Einhaltung dieser Bestimmungen abfragen, müssen aber unabhängig vom Alter einer Person einige nützliche Funktionen oder einen Unterhaltungswert umfassen.

Apps, die in erster Linie für Kinder gedacht sind, dürfen keine Analysen oder Werbung von Dritten enthalten. Das ermöglicht ein sichereres Erlebnis für Kinder.

(b) In vereinzelten Fällen sind Analysen und Werbung von Dritten unter Umständen zulässig, vorausgesetzt, dass die Dienste die gleichen Bedingungen wie in Richtlinie 1.3 einhalten.

Darüber hinaus müssen Apps in der Kategorie „Kinder“ oder Apps, die personenbezogene Daten (z. B. Name, Adresse, E-Mail-Adresse, Standort, Fotos, Videos, Zeichnungen, Chatmöglichkeiten, andere personenbezogene Daten oder dauerhafte Bezeichner, die in Kombination mit den oben genannten Elementen verwendet werden) von einem Minderjährigen erfassen, übertragen oder teilen können, eine Datenschutzrichtlinie enthalten und alle geltenden Datenschutzbestimmungen für Kinder einhalten. Aus Gründen der Genauigkeit entsprechen die Anforderungen an die Kontrollfunktionen für Eltern, die für die Kategorie „Kinder“ gelten, im Allgemeinen nicht dem im Rahmen dieser Datenschutzgesetze erforderlichen Einholen der elterlichen Zustimmung zur Erfassung persönlicher Daten des Kindes.

Zur Erinnerung: Richtlinie 2.3.8 erfordert, dass die Verwendung von Ausdrücken wie „Für Kinder“ in den App-Metadaten der Kategorie „Kinder“ vorbehalten ist. Apps, die nicht zur Kategorie „Kinder“ gehören, dürfen keine Begriffe in App-Namen, Untertiteln, Symbolen, Bildschirmfotos oder Beschreibungen enthalten, die darauf hindeuten, dass Kinder die Hauptzielgruppe der App sind.

5.1.5 Ortungsdienste

Verwenden Sie Ortungsdienste nur dann in Ihrer App, wenn sie unmittelbar für die Features und Dienste der App relevant sind. Standortbasierte APIs dürfen nicht für Notdienste oder die autonome Steuerung von Fahrzeugen, Flugzeugen und anderen Fahrzeugen verwendet werden, mit Ausnahme kleiner Geräte wie leichte Drohnen und Spielzeug oder ferngesteuerte Autoalarmsysteme usw. Stellen Sie sicher, dass Sie die Nutzer:innen informieren und ihre Einwilligung einholen, bevor Sie Standortdaten erfassen, übertragen oder verwenden. Wenn in Ihrer App Ortungsdienste verwendet werden, müssen Sie deren Zweck in Ihrer App erläutern. In den Human Interface Guidelines (Richtlinien für Nutzerschnittstellen) finden Sie bewährte Vorgehensweisen.

5.2 Geistiges Eigentum

Achten Sie darauf, dass Ihre App nur Inhalte enthält, die Sie erstellt haben oder für die Sie eine Lizenz haben. Ihre App wird möglicherweise entfernt, wenn Sie die rote Linie überschritten und Inhalte ohne Erlaubnis verwendet haben. Das bedeutet natürlich auch, dass die App einer anderen Person entfernt werden kann, wenn sie sich bei Ihnen „bedient“ hat. Sollten Sie der Ansicht sein, dass Ihre Urheberrechte durch eine:n andere:n Entwickler:in im App Store verletzt wurden, machen Sie Ihren Anspruch über das Webformular geltend. Die Gesetze sind je nach Land und Region verschieden, doch zumindest die folgenden häufigen Fehler sollten Sie vermeiden:

5.2.1 Allgemeines: Verwenden Sie in Ihrer App ohne Erlaubnis kein geschütztes Material von Dritten wie Markenzeichen, urheberrechtlich geschützte Werke oder patentierte Ideen und fügen Sie keine irreführenden, falschen oder nachahmenden Darstellungen, Namen oder Metadaten in Ihr App-Paket oder Ihren Entwicklernamen ein. Apps müssen von der natürlichen oder juristischen Person eingereicht werden, die im Besitz der Urheberrechte und anderer geltender Rechte ist oder diese lizenziert hat.

5.2.2 Websites/Dienste von Dritten: Wenn Ihre App Inhalte eines Dritten verwendet, auf diese zugreift, diese monetarisiert oder Inhalte aus dem Service eines Dritten anzeigt, müssen Sie sicherstellen, dass Ihnen das gemäß den Nutzungsbedingungen des Diensts ausdrücklich gestattet ist. Die Erlaubnis muss auf Anfrage vorgelegt werden.

5.2.3 Audio-/Videodownloads: Apps dürfen keine illegale Dateifreigabe ermöglichen oder die Möglichkeit zum Sichern, Konvertieren oder Laden von Medien von Dritten (z. B. Apple Music, YouTube, SoundCloud, Vimeo usw.) bieten, wenn nicht die ausdrückliche Genehmigung dieser Quellen vorliegt. Auch das Streamen von Audio-/Videoinhalten verstößt unter Umständen gegen die Nutzungsbedingungen. Beachten Sie das also, bevor Ihre App auf diese Dienste zugreift.
Die Erlaubnis muss auf Anfrage vorgelegt werden.

5.2.4 Zusicherungen von Apple:

(a) Sie dürfen nicht behaupten oder andeuten, dass Apple die Quelle oder der Anbieter der App ist oder dass Apple eine bestimmte Zusicherung bezüglich der Qualität oder Funktionalität macht.

(b) Wird Ihre App als „Editor's Choice“ ausgewählt, wendet Apple das Badge automatisch an.

5.2.5 Apple Produkte Erstellen Sie keine Apps, die bestehenden Apple Produkten, Oberflächen (z. B. Finder), Apps (z. B. App Store, iTunes Store oder Nachrichten) oder Werbethemen verwirrend ähneln. Apps und Erweiterungen, einschließlich Tastaturen und Stickerpakete von Dritten, enthalten möglicherweise kein Apple Emoji. Musik aus Vorschauen von iTunes und Apple Music darf nicht als Unterhaltungswert (z. B. als Hintergrundmusik für eine Fotocollage oder als Soundtrack für ein Spiel) oder auf andere nicht autorisierte Weise verwendet werden. Wenn Sie Musikvorschauen aus iTunes oder Apple Music bereitstellen, müssen Sie einen Link zu der entsprechenden Musik in iTunes oder Apple Music anzeigen. Wenn Ihre App Aktivitätsringe anzeigt, dürfen diese keine Bewegungs-, Trainings- oder Stehdaten auf eine Weise visualisieren, die dem Aktivitätssteuerelement ähnelt. In den Human Interface Guidelines (Richtlinien für Nutzerschnittstellen) erfahren Sie mehr über die Verwendung von Aktivitätsringen. Wenn Ihre App Apple Wetterdaten anzeigt, muss sie die Attributionsanforderungen in der Dokumentation für WeatherKit erfüllen.

5.3 Spiele, Glücksspiel und Lotterien

Spiele, Glücksspiele und Lotterien sind unter Umständen schwer zu verwalten und gehören zu den am stärksten regulierten Angeboten im App Store. Integrieren Sie diese Funktion nur, wenn Sie Ihre gesetzlichen Verpflichtungen überall dort, wo Sie Ihre App bereitstellen, eingehend geprüft haben und auf den zusätzlichen Zeitaufwand während der Überprüfung vorbereitet sind. Die folgenden Dinge sollten Sie beachten:

5.3.1 Gewinnspiele und Wettbewerbe müssen von den Entwickler:innen der App gesponsert werden.

5.3.2 Offizielle Regeln für Gewinnspiele, Wettbewerbe und Verlosungen müssen in der App dargestellt werden und deutlich machen, dass Apple kein Sponsor oder in irgendeiner Weise an der Aktivität beteiligt ist.

5.3.3 Apps dürfen keine In-App-Käufe verwenden, um Guthaben oder Währung für die Verwendung in Verbindung mit Echtgeldspielen jeglicher Art zu kaufen.

5.3.4 Apps, die Echtgeldspiele (z. B. Sportwetten, Poker, Casinospiele, Pferderennen) oder Lotterien anbieten, müssen über die erforderlichen Lizenzen und Berechtigungen an den Standorten verfügen, an denen die App verwendet wird, müssen geografisch auf diese Standorte beschränkt werden und müssen im App Store kostenlos sein. Illegale Spielhilfen, einschließlich Kartenzähler, sind im App Store nicht erlaubt. Lotterie-Apps müssen einen Einsatz, eine:n zufällig gewählte:n Gewinner:in und einen Preis bieten.

5.4 VPN-Apps

Apps, die VPN-Dienste anbieten, müssen die NEVPNManager API verwenden und dürfen nur von Entwickler:innen angeboten werden, die als Organisation registriert sind. Sie müssen eindeutig angeben, welche Nutzerdaten erfasst und wie sie auf einem App-Bildschirm vor Aktionen von Nutzer:innen (Kauf oder anderweitige Verwendung des Dienstes) verwendet werden. Apps, die VPN-Dienste anbieten, dürfen Dritten keine Daten zu einem beliebigen Zweck verkaufen, verwenden oder offenlegen und müssen sich dazu in ihrer Datenschutzrichtlinie verpflichten. VPN-Apps dürfen nicht gegen lokale Gesetze verstoßen. Wenn Sie Ihre VPN-App in einem Gebiet zur Verfügung stellen möchten, das eine VPN-Lizenz erfordert, müssen Sie die Lizenzinformationen in den Notizen für App Review angeben. Auch zugelassene Apps für die Kindersicherung, Inhaltssperren und die Sicherheit dürfen die NEVPNManager API verwenden. Apps, die diese Richtlinie nicht einhalten, werden aus dem App Store entfernt und für die Installation über die alternative Verteilung gesperrt, und Sie werden unter Umständen aus dem Apple Developer Program entfernt.

5.5 Mobile Geräteverwaltung

Apps für die mobile Geräteverwaltung, die Dienste für die mobile Geräteverwaltung (MDM-Dienste) anbieten, müssen diese Funktion bei Apple anfordern. Derartige Apps dürfen nur von kommerziellen Unternehmen, Bildungseinrichtungen oder Regierungsbehörden und in Einzelfällen von Unternehmen angeboten werden, die MDM für Kindersicherungsdienste oder die Gerätesicherheit verwenden. Sie müssen eindeutig angeben, welche Nutzerdaten erfasst und wie sie auf einem App-Bildschirm vor Aktionen von Nutzer:innen (Kauf oder anderweitige Verwendung des Dienstes) verwendet werden. MDM-Apps dürfen nicht gegen geltende Gesetze verstoßen. Apps, die MDM-Dienste anbieten, dürfen Dritten keine Daten zu einem beliebigen Zweck verkaufen, verwenden oder offenlegen und müssen sich dazu in ihrer Datenschutzrichtlinie verpflichten. In eingeschränkten Fällen sind Analysen von Dritten zulässig, sofern die Dienste nur Daten über die Leistung der MDM-App der Entwickler:innen erfassen oder übertragen und keine Daten über Nutzer:innen, das Gerät von Nutzer:innen oder andere auf diesem Gerät verwendete Apps. Apps, die Konfigurationsprofile anbieten, müssen diese Anforderungen ebenfalls erfüllen. Apps, die diese Richtlinie nicht einhalten, werden aus dem App Store entfernt und für die Installation über die alternative Verteilung gesperrt, und Sie werden unter Umständen aus dem Apple Developer Program entfernt.

5.6 Verhaltenskodex für Entwickler:innen

Bitte behandeln Sie alle mit Respekt, sei es in Ihren Antworten auf Rezensionen aus dem App Store, in Kundensupportanfragen oder in der Kommunikation mit Apple sowie in Ihren Antworten in App Store Connect. Belästigungen jeglicher Art, Diskriminierung, Einschüchterung, Mobbing und die Aufforderung anderer dazu sind nicht zulässig. Wiederholtes manipulatives oder irreführendes Verhalten oder andere betrügerische Handlungen führen dazu, dass Sie aus dem Apple Developer Program entfernt werden.

Kundenvertrauen ist ein Eckpfeiler des App-Ökosystems. Apps dürfen niemals Nutzer:innen ausnutzen oder versuchen, Kund:innen abzuzocken, sie dazu zu bringen, unerwünschte Käufe zu tätigen, sie dazu zu zwingen, unnötige Daten zu teilen, Preise auf irreführende Weise zu erhöhen, Features oder Inhalte in Rechnung zu stellen, die nicht bereitgestellt wurden, oder andere manipulative Praktiken innerhalb oder außerhalb der App durchzuführen.

Ihr Account für das Developer Program wird gekündigt, wenn Sie Aktivitäten oder Aktionen durchführen, die nicht dem Verhaltenskodex für Entwickler:innen entsprechen. Um Ihren Account wiederherzustellen, dürfen Sie eine schriftliche Erklärung abgeben, in der die geplanten Verbesserungen aufgeführt sind. Wenn Ihr Plan von Apple genehmigt wird und wir überprüft haben, dass die Änderungen vorgenommen wurden, kann Ihr Account wiederhergestellt werden.

5.6.1 Rezensionen im App Store

Kundenrezensionen im App Store sind ein integraler Bestandteil des App-Erlebnisses. Sie sollten Kund:innen also respektvoll behandeln, wenn Sie auf ihre Kommentare antworten. Achten Sie darauf, dass Ihre Antworten auf die Kommentare der Nutzer:innen ausgerichtet sind und keine persönlichen Informationen, Spam oder Marketing enthalten.

Verwenden Sie die bereitgestellte API, um Nutzer:innen aufzufordern, Ihre App zu überprüfen. Mit dieser Funktion können Kund:innen Bewertungen und Rezensionen im App Store abgeben, ohne die App verlassen zu müssen. Individuelle Aufforderungen zur Überprüfung sind nicht zulässig.

5.6.2 Identität von Entwickler:innen

Für das Kundenvertrauen ist es entscheidend, dass für Apple und die Kund:innen nachprüfbare Informationen bereitgestellt werden. Die Darstellung Ihrer Person, Ihres Unternehmens und Ihrer Angebote im App Store oder auf alternativen App-Marktplätzen muss korrekt sein. Die bereitgestellten Informationen müssen wahrheitsgemäß, relevant und aktuell sein, sodass Apple und Kund:innen verstehen, mit wem sie es zu tun haben, und Sie bei Problemen kontaktieren können.

5.6.3 Betrug

Die Teilnahme am App Store erfordert Integrität und die Bereitschaft, das Vertrauen der Kund:innen aufzubauen und zu bewahren. Die Manipulation von Elementen des Kundenerlebnisses im App Store, z. B. von Diagrammen, der Suche oder von Bewertungen oder Empfehlungen für Ihre App, minimiert das Vertrauen von Kund:innen und ist nicht zulässig.

5.6.4 App-Qualität

Kund:innen erwarten die höchste Qualität vom App Store und hochwertige Inhalte, Dienste und Erfahrungen fördern das Vertrauen von Kund:innen. Hinweise darauf, dass diese Erwartung nicht erfüllt wird, sind beispielsweise exzessive Kundenberichte zu Bedenken hinsichtlich Ihrer App, wie negative Kundenbewertungen und exzessive Erstattungsanfragen. Die Unfähigkeit, eine hohe Qualität aufrechtzuerhalten, kann ein Faktor bei der Entscheidung sein, ob Entwickler:innen den Verhaltenskodex einhalten.

Nach dem Einreichen

Wenn Sie Ihre App zusammen mit den Metadaten über App Store Connect eingereicht haben und Ihre App nun geprüft wird, berücksichtigen Sie bitte Folgendes:

- **Prüfdauer:** App Review überprüft Ihre App so schnell wie möglich. Wenn Ihre App jedoch komplex ist oder neue Probleme aufweist, kann dies eine gründlichere Untersuchung und Betrachtung erfordern. Wenn Ihre wiederholt aufgrund derselben Richtlinienverletzung abgelehnt wurde oder Sie versucht haben, das App Review-Verfahren zu manipulieren, wird Ihre App nicht weiter geprüft. Erfahren Sie mehr über App Review.

- **Statusaktualisierungen:** In App Store Connect können Sie den aktuellen Prüfstatus Ihrer App abfragen, sodass Sie stets auf dem neuesten Stand sind.

- **Eilanträge:** Wenn die Zeit knapp ist, können Sie ein beschleunigtes Prüfverfahren beantragen. Stellen Sie diese Eilanträge mit Rücksicht auf die anderen App-Entwickler:innen bitte nur, wenn es wirklich notwendig ist. Sollte sich herausstellen, dass Sie diese Option missbrauchen, lehnen wir künftige Anträge dieser Art ggf. ab.

- **Erscheinungsdatum:** Wenn das Erscheinungsdatum für Ihre App in der Zukunft liegt, wird sie erst ab diesem Datum im App Store angezeigt, auch wenn sie bereits vorher durch App Review zugelassen wurde. Vergessen Sie nicht, dass es bis zu 24 Stunden dauern kann, bis die App auf allen ausgewählten Store-Seiten angezeigt wird.

- **Ablehnungen:** Unser Ziel ist es, diese Richtlinien fair und konsistent anzuwenden, doch auch wir sind nicht perfekt. Wenn Ihre App abgelehnt wurde und Sie Fragen haben oder zusätzliches Material zur Verfügung stellen möchten, wenden Sie sich bitte über App Store Connect direkt an das App Review Team. So wird Ihre App vielleicht doch in den Store aufgenommen und uns bietet dies eine Möglichkeit, das App Review Verfahren zu verbessern und zu ermitteln, welcher Teil unserer Richtlinien vielleicht noch klarer formuliert werden muss.

- **Einspruch:** Wenn Sie dem Ergebnis einer Prüfung nicht zustimmen, legen Sie Einspruch ein. Die hilft Ihnen unter Umständen dabei, Ihre App im Store zu veröffentlichen. Sie können außerdem Änderungen an den Richtlinien selbst vorschlagen, um uns dabei zu helfen, den App Review-Prozess zu verbessern oder erforderliche Klarstellungen unserer Richtlinien zu ermitteln.

- **Einreichungen von Fehlerbehebungen:** Für Apps, die bereits im App Store oder auf einem alternativen App-Marktplatz vorhanden sind, werden Fehlerbehebungen bei Richtlinienverletzungen nicht verzögert (Ausnahme: bei rechtlichen oder Sicherheitsaspekten). Wenn Ihre App abgelehnt wurde und für diesen Prozess qualifiziert ist, wenden Sie sich bitte über App Store Connect direkt an das App Review Team. Geben Sie an, dass Sie diesen Prozess nutzen möchten und planen, dieses Problem bei der nächsten Einreichung anzugehen.

Wir freuen uns schon auf Ihre neuen Ideen!

Zuletzt aktualisiert: 5. April 2024