



Wytyczne Dotyczące Weryfikacji w App

Aplikacje zmieniają świat, wzbogacają życie ludzi i umożliwiają deweloperom takim jak Ty wprowadzanie innowacji, jak nigdy dotąd. W rezultacie App Store stał się ekscytującym i tętniącym życiem ekosystemem dla milionów deweloperów i ponad miliarda użytkowników. Niezależnie od tego, czy jesteś początkującym deweloperem, czy masz duży zespół doświadczonych programistów, cieszymy się, że tworzysz aplikacje na nasze platformy, i chcemy pomóc Ci w zrozumieniu naszych wytycznych, które dadzą Ci pewność, że Twoja aplikacja szybko przejdzie przez proces weryfikacji.

Marzec 2024 r.

Wprowadzenie	3
Przed zgłoszeniem	4
1. Bezpieczeństwo	5
1.1 Niewłaściwe treści	5
1.2 Treści generowane przez użytkowników	6
1.3 Kategoria Dzieci	7
1.4 Szkody fizyczne	8
1.5 Informacje o deweloperze	8
1.6 Bezpieczeństwo danych	9
1.7 Zgłaszanie działalności przestępczej	9
2. Wydajność	9
2.1 Kompletność aplikacji	9
2.2 Testy beta	9
2.3 Dokładne metadane	10
2.4 Zgodność sprzętu	12
2.5 Wymagania dotyczące oprogramowania	13
3. Model biznesowy	15
3.1 Płatności	16
3.2 Inne kwestie związane z modelem biznesowym	21
4. Projekt	22
4.1 Naśladownictwo	23
4.2 Minimalna funkcjonalność	23
4.3 Spam	24
4.4 Rozszerzenia	24
4.5 Witryny i usługi Apple	25
4.6 Alternatywne ikony aplikacji	26
4.7 Miniaplikacje, minigry, gry do strumieniowania, czatboty i wtyczki	27
4.8 Usługi logowania	27
4.9 Apple Pay	28
4.10 Zarabianie na wbudowanych funkcjach	28
5. Informacje prawne	29
5.1 Prywatność	29
5.2 Własność intelektualna	33
5.3 Gry, hazard i loterie	34
5.4 Aplikacje VPN	35
5.5 Zarządzanie urządzeniami mobilnymi	35
5.6 Kodeks postępowania deweloperów	35
Po zgłoszeniu	37

Wprowadzenie

Zasada przewodnia App Store jest prosta — chcemy zapewnić użytkownikom bezpieczne pobieranie aplikacji, a wszystkim deweloperom — możliwość odniesienia sukcesu. Realizujemy te cele, oferując starannie przygotowany App Store, w którym każda aplikacja jest weryfikowana przez ekspertów, a zespół redakcyjny pomaga użytkownikom codziennie odkrywać nowe aplikacje. Skanujemy również każdą aplikację pod kątem złośliwego oprogramowania i innych programów, które mogą mieć wpływ na bezpieczeństwo, zabezpieczenia i prywatność użytkowników. Dzięki tym staraniom platformy Apple stały się najbezpieczniejszymi miejscami udostępniającymi aplikacje dla konsumentów na całym świecie.

W Unii Europejskiej deweloperzy mogą również dystrybuować poświadczane aplikacje dla iOS za pośrednictwem alternatywnych platform sprzedaży aplikacji. Dowiedz się więcej o [alternatywnych platformach sprzedaży aplikacji](#) oraz [poświadczaniu aplikacji dla iOS](#). Aby sprawdzić, które wytyczne mają zastosowanie do poświadczania aplikacji dla iOS, kliknij opcję „Pokaż tylko wytyczne dotyczące weryfikacji poświadczania” w menu po lewej stronie.

Na wszystko inne zawsze pozostaje otwarty Internet. Jeśli model i wytyczne App Store albo alternatywne platformy sprzedaży aplikacji i poświadczanie aplikacji dla iOS nie są najlepsze dla Twojej aplikacji lub pomysłu na biznes, to nic nie szkodzi — udostępniamy przeglądarkę Safari, która również zapewnia wspaniały komfort korzystania z Internetu.

Na kolejnych stronach znajdziesz nasze najnowsze wytyczne podzielone na pięć przejrzystych sekcji: Bezpieczeństwo, Wydajność, Model biznesowy, Projekt i Informacje prawne. App Store stale się zmienia i ulepsza, aby nadążać za potrzebami naszych klientów i naszych produktów. Twoje aplikacje również powinny się zmieniać i ulepszać, aby pozostać w App Store.

Kilka innych kwestii dotyczących dystrybucji aplikacji na naszych platformach, o których należy pamiętać:

- Nasze aplikacje są często pobierane przez dzieci. Nadzór rodzicielski świetnie sprawdza się w ochronie dzieci, ale Ty też musisz zrobić swoje. Pamiętaj więc, że troszczymy się o bezpieczeństwo dzieci.
- App Store to świetny sposób na dotarcie do setek milionów ludzi na całym świecie. Jeśli tworzysz aplikację, którą chcesz po prostu pokazać rodzinie i znajomym, App Store nie jest do tego najlepszym miejscem. Rozważ użycie środowiska Xcode do bezpłatnej instalacji aplikacji na urządzeniu lub skorzystanie z dystrybucji ad hoc dostępnej dla członków programu Apple Developer Program. Jeśli dopiero zaczynasz, dowiedz się więcej o programie [Apple Developer Program](#).
- Zdecydowanie popieramy reprezentowanie wszystkich punktów widzenia w App Store, o ile aplikacje szanują użytkowników o odmiennych opiniach, a jakość korzystania z aplikacji jest świetna. Będziemy odrzucać aplikacje ze względu na wszelkie treści lub zachowania, które naszym zdaniem przekraczają granicę. Gdzie leży ta granica, zapytasz? Cóż, jak powiedział kiedyś sędzia Sądu Najwyższego: „Będę wiedział, gdy to zobaczę”. I sądzimy, że Ty również zrozumiesz moment przekroczenia takiej granicy.
- Jeśli spróbujesz oszukać system (na przykład próbując oszukać proces weryfikacji, wykraść dane użytkownika, skopiować pracę innego dewelopera, manipulować ocenami lub odkryciami w App Store), spowoduje to usunięcie Twoich aplikacji ze sklepu i wykluczenie Cię z programu Apple Developer Program.

- Odpowiadasz za to, by wszystko w Twojej aplikacji, w tym sieci reklamowe, usługi analityczne i pakiety SDK innych firm, było zgodne z tymi wytycznymi, więc sprawdzaj i wybieraj je uważnie.

- Niektóre funkcje i technologie, które nie są ogólnie dostępne dla deweloperów, mogą być oferowane jako uprawnienia dla ograniczonych przypadków użycia. Oferujemy na przykład uprawnienia do CarPlay Audio, HyperVisor i Privileged File Operations. Zapoznaj się z naszą dokumentacją na stronie developer.apple.com, aby dowiedzieć się więcej na temat uprawnień.

Mamy nadzieję, że te wytyczne pomogą Ci gładko przejść przez proces weryfikacji i że zatwierdzenia oraz odrzucenia będą spójne we wszystkich przypadkach. Dokument ten może ulegać zmianom; nowe aplikacje przedstawiające nowe pytania mogą w dowolnym momencie skutkować zmianą zasad. Być może to właśnie Twoja aplikacja doprowadzi do zmian. Uwielbiamy naszą pracę i szanujemy to, co robisz. Dokładamy wszelkich starań, aby stworzyć najlepszą na świecie platformę, która pozwoli Ci wyrazić swoje talenty i przy okazji zarobić na życie.

Przed zgłoszeniem

Aby zatwierdzenie aplikacji przebiegło jak najsprawniej, zapoznaj się z wymienionymi poniżej typowymi błędami, które mogą spowolnić proces weryfikacji lub spowodować odrzucenie aplikacji. Nie zastępuje to wytycznych ani nie gwarantuje, że aplikacja zostanie zatwierdzona, ale upewnienie się, że możesz odhaczyć każdą pozycję na liście, to dobry początek. Jeśli aplikacja nie działa zgodnie z przeznaczeniem lub jej już aktywnie nie wspierasz, zostanie usunięta z App Store. [Dowiedz się więcej o udoskonaleniach App Store.](#)

Wykonaj następujące czynności:

- Przetestuj aplikację pod kątem awarii i błędów
- Upewnij się, że wszystkie informacje i metadane aplikacji są kompletne i dokładne
- Uaktualnij swoje dane kontaktowe na wypadek, gdyby zespół App Review musiał się z Tobą skontaktować
- Zapewnij zespołowi App Review pełny dostęp do aplikacji. Jeśli aplikacja zawiera funkcje powiązane z kontem, podaj aktywne konto demonstracyjne lub w pełni funkcjonalny tryb demonstracyjny, a także wszelki inny sprzęt lub zasoby, które mogą być potrzebne do weryfikacji aplikacji (np. dane logowania lub przykładowy kod QR)
- Włącz usługi zalecane, aby działały i były dostępne podczas weryfikacji
- Dołącz szczegółowe wyjaśnienia nieoczywistych funkcji i zakupów w aplikacji w uwagach do zespołu App Review, w tym — w stosownych przypadkach — dokumentację pomocniczą
- Sprawdź, czy aplikacja jest zgodna ze wskazówkami zawartymi w innych dokumentach, takich jak:

Development Guidelines (Wytyczne dotyczące tworzenia oprogramowania)

[UIKit](#)

[AppKit](#)

[WatchKit](#)

[App Extensions](#) (Rozszerzenia aplikacji)

[iOS Data Storage Guidelines](#) (Wytyczne dotyczące przechowywania danych w systemie iOS)

[Apple File System](#)

[App Store Connect Help](#) (Pomoc dotycząca App Store Connect)

[Developer Account Help](#) (Pomoc dotycząca konta dewelopera)



Design Guidelines (Wytyczne dotyczące projektowania)

[Human Interface Guidelines](#) (Wytyczne dotyczące interfejsu użytkownika)

Brand and Marketing Guidelines (Wytyczne dotyczące marki i marketingu)

[Marketing Resources and Identity Guidelines](#) (Materiały marketingowe i wytyczne dotyczących identyfikacji wizualnej)

[Apple Pay Marketing Guidelines](#) (Wytyczne marketingowe dotyczące usługi Apple Pay)

[Add to Apple Wallet Guidelines](#) (Wytyczne dotyczące dodawania rzeczy do Portfela Apple)

[Guidelines for Using Apple Trademarks and Copyrights](#) (Wytyczne dotyczące korzystania ze znaków towarowych i praw autorskich Apple)

Wytyczne zawierające  dotyczą [Poświadczenia aplikacji dla iOS](#) w UE.

1. Bezpieczeństwo

Gdy użytkownicy instalują aplikację ze sklepu App Store, chcą mieć pewność, że jest to bezpieczne — że aplikacja nie zawiera denerwujących lub obraźliwych treści, nie uszkodzi ich urządzeń, a w wyniku jej używania nie dojdzie do szkód fizycznych. Poniżej przedstawiliśmy główne pułapki, ale możemy od razu powiedzieć, że jeśli celem Twojej aplikacji jest szokowanie i obrażanie innych, App Store nie jest dla niej właściwym miejscem. Niektóre z tych zasad zostały również uwzględnione w poświadczeniu aplikacji dla iOS.

1.1 Niewłaściwe treści

Aplikacje nie powinny zawierać treści, które są obraźliwe, niedelikatne, denerwujące, mające na celu wywołanie odrazy, w wyjątkowo złym guście lub po prostu przerażające. Przykłady takich treści to:

1.1.1 Treści zniesławiające, dyskryminujące lub złośliwe, w tym odniesienia do lub komentarze na temat religii, rasy, orientacji seksualnej, płci, pochodzenia narodowego/etnicznego lub innych wybranych grup osób, szczególnie jeśli aplikacja może upokorzyć, zastraszyć lub skrzywdzić docelową osobę lub grupę. Zasadniczo wymóg ten nie dotyczy zawodowych satyryków i humorystów.

1.1.2 Realistyczne przedstawianie zabijanych, okaleczanych, torturowanych lub maltretowanych ludzi lub zwierząt, a także treści zachęcające do przemocy. Określenie „wrogowie” w kontekście gry nie może odnosić się wyłącznie do określonej rasy, kultury, prawdziwego urzędu, korporacji lub jakiegokolwiek innej rzeczywistej jednostki.

1.1.3 Przedstawienia zachęcające do nielegalnego lub lekkomyślnego użycia broni i niebezpiecznych przedmiotów bądź ułatwiający zakup broni palnej lub amunicji.

1.1.4 Materiały jawnie seksualne lub pornograficzne, definiowane jako „wyraźne opisy lub pokazy narządów płciowych albo czynności mających na celu pobudzenie uczuć erotycznych, a nie estetycznych czy emocjonalnych”. Obejmuje to aplikacje erotyczne typu „hookup” oraz inne aplikacje, które mogą zawierać pornografię lub być wykorzystywane do ułatwiania prostytucji bądź handlu ludźmi i ich wykorzystywania.

1.1.5 Podżegające komentarze religijne albo niedokładne lub wprowadzające w błąd cytaty z tekstów religijnych.

1.1.6 ↻ Fałszywe informacje i funkcje, w tym nieprawdziwe dane urzędzenia lub sztuczki/żarty, takie jak fałszywe lokalizatory. Stwierdzenie, że aplikacja służy „do celów rozrywkowych”, nie znosi tej wytycznej. Aplikacje, które umożliwiają anonimowe lub żartobliwe rozmowy telefoniczne lub wysyłanie wiadomości SMS/MMS, będą odrzucane.

1.1.7 Szkodliwe koncepcje, które wykorzystują lub próbują wykorzystać ostatnie lub aktualne wydarzenia, takie jak gwałtowne konflikty, ataki terrorystyczne i epidemie.

1.2 Treści generowane przez użytkowników

Aplikacje zawierające treści generowane przez użytkowników rodzą szczególne wyzwania — od naruszenia własności intelektualnej po anonimowe prześladowanie. Aby zapobiec nadużyciom, aplikacje z treściami generowanymi przez użytkowników lub usługi sieci społecznościowych muszą zawierać:

- Metodę filtrowania niewłaściwych treści przed publikowaniem ich w aplikacji
- Mechanizm zgłaszania obraźliwych treści i szybkiego reagowania na wątpliwości
- Możliwość blokowania nieuczciwym użytkownikom dostępu do usługi
- Opublikowane informacje kontaktowe, aby użytkownicy mogli łatwo się z Tobą skontaktować

Aplikacje z treściami lub usługami generowanymi przez użytkowników, które ostatecznie są wykorzystywane głównie do celów pornograficznych, kontaktów w stylu Chatroulette, uprzedmiotowienia prawdziwych osób (np. głosowania typu „hot-or-not”), kierowania gróźb fizycznych lub prześladowania, nie mają racji bytu w App Store i mogą zostać usunięte bez uprzedzenia. Jeśli aplikacja zawiera treści

generowane przez użytkowników z usługi internetowej, może wyświetlać incydentalne treści typu „NSFW” przeznaczone dla dorosłych, pod warunkiem, że treści te są domyślnie ukryte i wyświetlane tylko wtedy, gdy użytkownik włączy je za pośrednictwem Twojej witryny.

1.2.1 Treści od twórców

Aplikacje, które zawierają treści od określonej społeczności użytkowników, zwanej „twórcami”, są świetną sprawą, jeśli są odpowiednio moderowane. Aplikacje te zapewniają klientom wyjątkowe, ujednolicone środowisko interakcji z różnymi rodzajami treści od twórców. Oferują narzędzia i programy, które pomagają tej społeczności twórców niebędących deweloperami w tworzeniu, udostępnianiu i monetyzowaniu doświadczeń generowanych przez użytkowników. Środowiska te nie mogą zmieniać podstawowych cech i funkcjonalności aplikacji natywnej, a raczej dodają treść do tych ustrukturyzowanych środowisk. Te środowiska nie są natywnymi „aplikacjami” zakodowanymi przez deweloperów — są one treścią w samej aplikacji i są przez zespół App Review traktowane jako treści generowane przez użytkowników. Takie treści od twórców mogą obejmować filmy, artykuły, nagrania audio, a nawet gry casual. App Store obsługuje aplikacje oferujące takie treści generowane przez użytkowników, o ile są one zgodne ze wszystkimi Wytycznymi, w tym z Wytycznymi 1.2 dotyczącymi moderowania treści generowanych przez użytkowników oraz Wytycznymi 3.1.1 dotyczącymi płatności i zakupów w aplikacji. Aplikacje oferujące treści od twórców powinny mieć taką samą klasyfikację wiekową jak najwyżej sklasyfikowane pod względem wiekowym treści dostępne w aplikacji oraz informować użytkowników, które treści wymagają dodatkowych zakupów.

1.3 Kategoria Dzieci

Kategoria Dzieci to świetny sposób na łatwe znajdowanie aplikacji przeznaczonych dla dzieci. Jeśli chcesz brać udział w kategorii Dzieci, Twoje działania powinny skupiać się na tworzeniu wspaniałych doświadczeń specjalnie dla młodszych użytkowników. Aplikacje te nie mogą zawierać łączy wychodzących z aplikacji, możliwości robienia zakupów ani innych elementów rozpraszających uwagę dzieci, chyba że są one zarezerwowane dla wyznaczonego obszaru za bramką rodzicielską. Pamiętaj, że jeśli klienci oczekują, że Twoja aplikacja spełnia wymagania kategorii Dzieci, będzie musiała nadal spełniać te wytyczne w kolejnych uaktualnieniach, nawet jeśli zdecydujesz się odznaczyć tę kategorię. Dowiedz się więcej o [urządzeniach do kontroli rodzicielskiej](#).

Musisz przestrzegać obowiązujących na całym świecie przepisów dotyczących prywatności związanych z gromadzeniem danych dzieci w Internecie. Zapoznaj się z [sekcją Prywatność](#) w niniejszych wytycznych, aby uzyskać więcej informacji. Ponadto aplikacje z kategorii Dzieci nie mogą wysyłać osobom trzecim informacji umożliwiających identyfikację osób ani informacji o urządzeniu. Aplikacje z kategorii Dzieci nie powinny zawierać narzędzi analitycznych ani reklam stron trzecich. Zapewnia to bezpieczniejsze doświadczenia dla dzieci. W niektórych przypadkach narzędzia analityczne stron trzecich mogą być dozwolone pod warunkiem, że usługi nie zbierają ani nie przekazują identyfikatorów IDFA ani żadnych informacji umożliwiających identyfikację dzieci (takich jak imię i nazwisko, data urodzenia, adres e-mail), ich lokalizacji lub informacji o urządzeniach. Obejmuje to wszelkie informacje o urządzeniu, sieci lub inne informacje, których można użyć bezpośrednio lub w połączeniu z innymi informacjami w celu identyfikacji użytkowników i ich urządzeń. W ograniczonych przypadkach mogą też być dozwolone reklamy kontekstowe stron trzecich, pod warunkiem, że usługi te mają publicznie udokumentowane praktyki i zasady dotyczące aplikacji z kategorii Dzieci, obejmujące wykonywaną przez człowieka weryfikację kreacji reklamowych pod kątem stosowności do wieku.

1.4 Szkody fizyczne

Jeśli aplikacja działa w sposób, który stwarza ryzyko szkód fizycznych, możemy ją odrzucić. Przykłady:

1.4.1 Aplikacje medyczne, które mogłyby dostarczać niedokładnych danych bądź informacji lub być wykorzystywane do diagnozowania bądź leczenia pacjentów, mogą być poddawane bardziej szczegółowej weryfikacji.

- Aplikacje muszą wyraźnie ujawnić dane i metodologię na poparcie twierdzeń dotyczących dokładności pomiarów zdrowotnych, a jeśli poziom dokładności lub metodologia nie mogą zostać potwierdzone, aplikacja zostanie odrzucona. Na przykład niedozwolone są aplikacje, które deklarują, że wykonują zdjęcia rentgenowskie, mierzą ciśnienie krwi, temperaturę ciała, poziom glukozy we krwi lub poziom tlenu we krwi przy użyciu wyłącznie czujników znajdujących się w urządzeniu.

- Aplikacje powinny przypominać użytkownikom, aby oprócz korzystania z aplikacji i przed podjęciem decyzji medycznych skonsultowali się z lekarzem.

Jeśli Twoja aplikacja medyczna uzyskała zgodę organów regulacyjnych, prześlij łącze do tej dokumentacji wraz z aplikacją.

1.4.2 Kalkulatory dawkowania leków muszą pochodzić od producenta leku, szpitala, uniwersytetu, firmy ubezpieczeń zdrowotnych, apteki lub innego zatwierzonego podmiotu bądź uzyskać zgodę agencji FDA lub jednego z jej międzynarodowych odpowiedników. Biorąc pod uwagę potencjalne szkody dla pacjentów, musimy mieć pewność, że aplikacja będzie wspierana i uaktualniana przez dłuższy czas.

1.4.3 Aplikacje zachęcające do spożywania wyrobów tytoniowych i e-papierosów, nielegalnych narkotyków lub nadmiernych ilości alkoholu nie są dozwolone. Aplikacje zachęcające nieletnich do spożywania którejkolwiek z tych substancji będą odrzucane. Ułatwianie sprzedaży substancji kontrolowanych (z wyjątkiem licencjonowanych aptek i licencjonowanych lub w inny sposób legalnych punktów sprzedaży konopi) lub tytoniu jest niedozwolone.

1.4.4 Aplikacje mogą wyświetlać tylko punkty kontroli trzeźwości opublikowane przez organy ścigania i nigdy nie powinny zachęcać do jazdy pod wpływem alkoholu ani innych brawurowych zachowań, takich jak nadmierna prędkość.

1.4.5 Aplikacje nie powinny nakłaniać klientów do udziału w działaniach (takich jak zakłady, wyzwania itp.) lub korzystania z urządzeń w sposób, który grozi fizyczną szkodą dla nich samych lub innych osób.

1.5 Informacje o deweloperze

Użytkownicy muszą wiedzieć, jak się z Tobą skontaktować w przypadku pytań i problemów wymagających wsparcia. Upewnij się, że Twoja aplikacja i jej adres URL wsparcia zawierają łatwy sposób skontaktowania się z Tobą; jest to szczególnie ważne w przypadku aplikacji, które mogą być używane w klasach. Brak dokładnych i aktualnych informacji kontaktowych nie tylko frustruje klientów, ale może też stanowić naruszenie prawa w niektórych krajach lub regionach. Upewnij się też, że karty w aplikacji Portfel zawierają prawidłowe dane kontaktowe od wydawcy i są podpisane specjalnym certyfikatem przypisanym do marki lub znaku towarowego karty.

1.6 Bezpieczeństwo danych ↩️

Aplikacje powinny wdrażać odpowiednie środki bezpieczeństwa, aby zapewnić właściwe postępowanie z informacjami o użytkownikach zebranymi zgodnie z umową licencyjną programu Apple Developer Program oraz niniejszymi Wytycznymi (więcej informacji można znaleźć w Wytycznych 5.1) oraz zapobiegać nieautoryzowanemu użyciu, ujawnianiu lub dostępowi do tych informacji przez strony trzecie.

1.7 Zgłaszanie działalności przestępczej

Aplikacje do zgłaszania domniemanej działalności przestępczej muszą angażować lokalne organy ścigania i mogą być oferowane wyłącznie w krajach lub regionach, w których takie zaangażowanie jest aktywne.

2. Wydajność

2.1 Kompletność aplikacji

Aplikacje zgłaszane do weryfikacji, w tym aplikacje udostępniane do zamówienia w przedsprzedaży, powinny być ostatecznymi wersjami ze wszystkimi niezbędnymi metadanymi i w pełni funkcjonalnymi adresami URL. Tekst zastępczy, puste strony internetowe i inne tymczasowe treści należy wyczyścić przed zgłoszeniem. Przed zgłoszeniem aplikacji upewnij się, że została ona przetestowana na urządzeniu pod kątem błędów i stabilności. Dołącz też informacje o koncie demonstracyjnym (i włącz usługę zaplecza!), jeśli aplikacja obejmuje logowanie. Jeśli ze względu na zobowiązania prawne lub związane z bezpieczeństwem nie możesz zapewnić konta demonstracyjnego, możesz w zamian włączyć wbudowany tryb demonstracyjny za uprzednią zgodą Apple. Upewnij się, że tryb demonstracyjny prezentuje pełne możliwości i funkcjonalność aplikacji. Jeśli aplikacja oferuje zakupy w aplikacji, upewnij się, że są one kompletne, aktualne i widoczne dla osoby weryfikującej, a jeśli takie nie są, wyjaśnij to w uwagach do weryfikacji. Nie traktuj weryfikacji aplikacji jako usługi testowania oprogramowania. Będziemy odrzucać niekompletne pakiety aplikacji i pliki binarne, które ulegają awariom lub wykazują oczywiste problemy techniczne.

2.2 Testy beta

App Store nie jest miejscem na wersje demonstracyjne, beta i próbne — zamiast tego użyj aplikacji TestFlight. Każda aplikacja przesłana do dystrybucji beta za pośrednictwem TestFlight powinna być przeznaczona do publicznej dystrybucji i powinna być zgodna z Wytycznymi Dotyczącymi Weryfikacji Aplikacji. Należy jednak pamiętać, że aplikacje korzystające z TestFlight nie mogą być dystrybuowane wśród testerów w zamian za jakiegokolwiek wynagrodzenie, w tym jako nagroda za finansowanie społecznościowe. Istotne uaktualnienia wersji beta należy przesłać do działu TestFlight App Review, zanim zostaną rozesłane do testerów. Więcej informacji znajdziesz na stronie [TestFlight Beta Testing](#) (Testy beta TestFlight).

2.3 Dokładne metadane ↗

Klienci powinni wiedzieć, co otrzymują, gdy pobierają lub kupują Twoją aplikację, więc upewnij się, że wszystkie metadane aplikacji, w tym informacje o prywatności, opis aplikacji, zrzuty ekranu i podglądy, dokładnie odzwierciedlają podstawowe funkcje aplikacji, i pamiętaj, aby uaktualniać je w miarę pojawiania się nowych wersji.

2.3.1

(a) ↗ Nie umieszczaj w swojej aplikacji żadnych ukrytych, nieaktywnych ani nieudokumentowanych funkcji. Funkcjonalność aplikacji powinna być jasna dla użytkowników końcowych i zespołu App Review. Wszystkie nowe cechy, funkcjonalności i zmiany produktu muszą być opisane w sposób szczegółowy w sekcji Notes for Review (Uwagi do weryfikacji) w App Store Connect (opisy ogólne będą odrzucane) i dostępne do weryfikacji. Podobnie marketing aplikacji w sposób wprowadzający w błąd, na przykład przez promowanie treści lub usług, których aplikacja w rzeczywistości nie oferuje (np. skanerów wirusów i złośliwego oprogramowania opartych na systemie iOS), lub promowanie fałszywej ceny, zarówno w ramach App Store, jak i poza nim, stanowi podstawę do usunięcia aplikacji z App Store lub blokady jej instalacji za pośrednictwem alternatywnego kanału dystrybucji oraz do zamknięcia konta dewelopera.

(b) Rażące lub powtarzające się zachowanie jest podstawą do usunięcia z programu Apple Developer Program. Ciężko pracujemy nad tym, aby App Store był ekosystemem godnym zaufania i oczekujemy, że nasi twórcy aplikacji będą postępować podobnie. Nie chcemy robić z interesów z nieuczciwymi osobami.

2.3.2 Jeśli aplikacja obejmuje zakupy w aplikacji, upewnij się, że opis, zrzuty ekranu i podglądy aplikacji jasno wskazują, czy są jakieś polecane przedmioty, poziomy, subskrypcje itp. wymagające dodatkowych zakupów. Jeśli zdecydujesz się promować zakupy w aplikacji w App Store, upewnij się, że nazwa wyświetlana, zrzut ekranu i opis zakupu w aplikacji są odpowiednie dla odbiorców publicznych, że postępujesz zgodnie ze wskazówkami zawartymi w artykule [Promoting Your In-App Purchases](#) (Promowanie zakupów w aplikacji) oraz że aplikacja poprawnie obsługuje [metodę SKPaymentTransactionObserver](#), aby klienci mogli bezproblemowo sfinalizować zakup po uruchomieniu aplikacji.

2.3.3 Zrzuty ekranu powinny przedstawiać aplikację w trakcie jej używania, a nie tylko grafikę tytułową, stronę logowania lub ekran powitalny. Mogą również zawierać nakładki tekstowe i graficzne (np. w celu zademonstrowania mechanizmów wprowadzania danych, takich jak animowany punkt dotyku lub Apple Pencil) i prezentować rozszerzone funkcje urządzenia, takie jak pasek Touch Bar.

2.3.4 Podglądy to dla klientów świetny sposób zobaczenia, jak wygląda Twoja aplikacja i co robi. Aby użytkownicy wiedzieli, co otrzymają wraz z aplikacją, podglądy mogą zawierać tylko zrzuty ekranu z wideo z samej aplikacji. Naklejki i rozszerzenia iMessage mogą przedstawiać doświadczenie użytkownika w aplikacji Wiadomości. Możesz dodać narrację i wideo lub nakładki tekstowe, aby wyjaśnić wszystko, co nie jest jasne na podstawie samego wideo.

2.3.5 ↗ Wybierz kategorię najbardziej odpowiednią dla swojej aplikacji, a jeśli potrzebujesz pomocy, zapoznaj się z [definicjami kategorii w App Store](#). Jeśli nie możesz trafić w żadną kategorię, możemy zmienić kategorię za Ciebie.

2.3.6 ➡ Odpowiedz szczerze na pytania dotyczące klasyfikacji wiekowej w App Store Connect, aby Twoja aplikacja była prawidłowo dopasowana do nadzoru rodzicielskiego. Jeśli aplikacja zostanie źle sklasyfikowana, klienci mogą być zaskoczeni tym, co dostają, lub może to wywołać zapytanie od organów regulacyjnych. Jeśli aplikacja zawiera multimedia, które wymagają wyświetlania klasyfikacji treści lub ostrzeżeń (np. filmy, muzykę, gry itp.), odpowiadasz za przestrzeganie lokalnych wymagań na każdym terytorium, na którym aplikacja jest dostępna.

2.3.7 ➡ Wybierz unikalną nazwę aplikacji, przypisz słowa kluczowe, które dokładnie opisują aplikację, i nie próbuj umieszczać w żadnych metadanych haseł będących znakami towarowymi, popularnych nazw aplikacji, informacji o cenach ani innych nieistotnych fraz tylko po to, aby oszukać system. Nazwy aplikacji mogą mieć maksymalnie 30 znaków. Metadane, takie jak nazwy aplikacji, napisy, zrzuty ekranu i podglądy, nie powinny zawierać cen, warunków ani opisów, które nie są charakterystyczne dla danego typu metadanych. Napisy w aplikacji to świetny sposób na zapewnienie dodatkowego kontekstu dla aplikacji. Muszą być zgodne z naszymi standardowymi zasadami dotyczącymi metadanych i nie powinny zawierać nieodpowiednich treści, odwoływać się do innych aplikacji ani zawierać niemożliwych do zweryfikowania oświadczeń dotyczących produktów. Apple może w dowolnym momencie zmodyfikować nieodpowiednie słowa kluczowe lub podjąć inne odpowiednie kroki, aby zapobiec nadużyciom.

2.3.8 ➡ Metadane powinny być odpowiednie dla wszystkich odbiorców, więc upewnij się, że ikony aplikacji i zakupów w aplikacji, zrzuty ekranu oraz podglądy są zgodne z klasyfikacją wiekową 4+, nawet jeśli aplikacja ma wyższą klasyfikację. Na przykład jeśli aplikacja jest grą, która zawiera przemoc, wybierz obrazy, które nie przedstawiają makabrycznej śmierci ani broni wycelowanej w konkretną postać. Używanie w metadanych aplikacji określeń takich jak „Dla dzieci” jest w App Store zastrzeżone dla kategorii Dzieci. Pamiętaj, aby metadane, w tym nazwa aplikacji i ikony (mała, duża, aplikacja na Apple Watch, ikony alternatywne itp.), były podobne, aby uniknąć zamieszania.

2.3.9 Ponosisz odpowiedzialność za zabezpieczenie praw do korzystania ze wszystkich materiałów w ikonach, zrzutach ekranu i podglądach aplikacji, a zamiast danych prawdziwej osoby musisz wyświetlać fikcyjne informacje o koncie.

2.3.10 Upewnij się, że Twoja aplikacja jest ukierunkowana na środowisko iOS, iPadOS, macOS, tvOS lub watchOS, i nie umieszczaj nazw, ikon ani obrazów innych platform mobilnych lub alternatywnych platform sprzedaży aplikacji w swojej aplikacji lub metadanych, chyba że istnieje określona, zatwierdzona funkcja interaktywna. Upewnij się, że metadane aplikacji dotyczą samej aplikacji i jej działania. Nie umieszczaj w nich nieistotnych informacji.

2.3.11 Aplikacje zgłaszane do zamówień w przedsprzedaży w App Store muszą być kompletne i możliwe do dostarczenia w takiej postaci, w jakiej zostały zgłoszone. Zadbaj o to, aby aplikacja, którą ostatecznie wydasz, nie różniła się zasadniczo od tej, którą reklamujesz, gdy aplikacja jest w stanie przedsprzedaży. Jeśli dokonasz istotnych zmian w aplikacji (np. zmienisz model biznesowy), musisz ponownie uruchomić sprzedaż w przedsprzedaży.

2.3.12 Aplikacje muszą jasno opisywać nowe funkcje i zmiany w produkcie w tekście „Co nowego”. Proste poprawki błędów, uaktualnienia zabezpieczeń i ulepszenia wydajności mogą polegać na ogólnym opisie, ale bardziej znaczące zmiany muszą być wymienione w uwagach.

2.3.13 Wydarzenia w aplikacji to wydarzenia, które odbywają się w określonym czasie w aplikacji. Aby wydarzenie było polecane w App Store, musi należeć do typu wydarzenia dostępnego w App Store Connect. Wszystkie metadane wydarzenia muszą być dokładne i odnosić się do samego wydarzenia, a nie ogólnie do aplikacji. Wydarzenia muszą odbywać się w godzinach i dniach wybranych w App Store Connect, w tym w wielu witrynach sklepowych. Możesz zarabiać na swoim wydarzeniu, o ile przestrzegasz zasad określonych w sekcji 3, zatytułowanej Model biznesowy. Precyzyjne łącze do wydarzenia musi kierować użytkowników do właściwego miejsca w aplikacji. Szczegółowe wskazówki dotyczące akceptowanych metadanych wydarzeń oraz precyzyjnych łączy do wydarzeń można znaleźć w artykule [In-App Events](#) (Wydarzenia w aplikacji).

2.4 Zgodność sprzętu

2.4.1 Aby użytkownicy mogli w pełni korzystać z możliwości aplikacji, aplikacje na iPhone'a powinny, jeśli tylko jest to możliwe, działać na iPadzie. Zachęcamy do rozważenia tworzenia uniwersalnych aplikacji, aby klienci mogli z nich korzystać na wszystkich swoich urządzeniach. Dowiedz się więcej o [aplikacjach uniwersalnych](#).

2.4.2 ➡ Zaprojektuj aplikację tak, aby była energooszczędna, a jej używanie nie groziło uszkodzeniem urządzenia. Aplikacje nie powinny gwałtownie rozładowywać baterii, generować nadmiernego ciepła ani niepotrzebnie obciążać zasobów urządzenia. Na przykład aplikacje nie powinny zachęcać do umieszczania urządzenia pod materacem lub poduszką podczas ładowania ani wykonywać nadmiernej liczby cykli zapisu na dysku półprzewodnikowym. Aplikacje, w tym wszelkie wyświetlane w nich reklamy stron trzecich, nie mogą uruchamiać niepowiązanych procesów w tle, takich jak wydobywanie kryptowalut.

2.4.3 Użytkownicy powinni mieć możliwość korzystania z aplikacji na Apple TV bez potrzeby korzystania ze sprzętu poza pilotem Siri Remote lub kontrolerami do gier stron trzecich, ale możesz swobodnie zapewniać rozszerzoną funkcjonalność, gdy są podłączone inne urządzenia peryferyjne. Jeśli wymagasz używania kontrolera do gier, pamiętaj, by jasno wyjaśnić to w metadanych, tak aby klienci wiedzieli, że do grania potrzebują dodatkowego sprzętu.

2.4.4 ➡ Aplikacje nigdy nie powinny sugerować ani wymagać ponownego uruchomienia urządzenia ani modyfikacji ustawień systemowych niezwiązanych z podstawowymi funkcjami aplikacji. Na przykład nie zachęcaj użytkowników do wyłączenia sieci Wi-Fi, wyłączenia funkcji zabezpieczeń itp.

2.4.5 Aplikacje dystrybuowane za pośrednictwem Mac App Store mają kilka dodatkowych wymagań, o których należy pamiętać:

(i) Muszą odpowiednio działać w piaskownicy i być zgodne z [dokumentacją systemu plików macOS](#). Powinny również używać odpowiednich interfejsów API systemu macOS do modyfikowania danych użytkownika przechowywanych przez inne aplikacje (np. zakładek, książki adresowej lub wpisów kalendarza).

(ii) Muszą być spakowane i przesłane przy użyciu technologii dostarczonych w środowisku Xcode; żadne instalatory stron trzecich nie są dozwolone. Muszą być również samodzielnymi pakietami instalacyjnymi pojedynczej aplikacji i nie mogą instalować kodu ani zasobów we współdzielonych lokalizacjach.

(iii) Nie mogą uruchamiać się automatycznie ani mieć innego kodu uruchamianego automatycznie podczas uruchamiania lub logowania bez zgody, ani nie mogą tworzyć procesów, które nadal działają bez zgody po zamknięciu aplikacji przez użytkownika. Nie powinny automatycznie dodawać swoich ikon do Docka ani pozostawiać skrótów na biurku użytkownika.

(iv) Nie mogą pobierać ani instalować samodzielnych aplikacji, rozszerzeń jądra, dodatkowego kodu ani zasobów w celu dodania funkcjonalności lub znaczącej zmiany aplikacji w stosunku do tego, co widzimy podczas procesu weryfikacji.

(v) Nie mogą żądać zwiększenia uprawnień do poziomu użytkownika root ani używać atrybutów setuid.

(vi) Nie mogą wyświetlać ekranu licencji podczas uruchamiania, wymagać kluczy licencyjnych ani wdrażać własnych zabezpieczeń przed kopiowaniem.

(vii) Do dystrybucji uaktualnień muszą używać Mac App Store; inne mechanizmy uaktualniania nie są dozwolone.

(viii) Aplikacje powinny działać w aktualnie oferowanym systemie operacyjnym i nie mogą korzystać z przestarzałych lub instalowanych opcjonalnie technologii (np. Java)

(ix) Aplikacje muszą zapewniać pełną obsługę języków i lokalizacji w jednym pakiecie aplikacji.

2.5 Wymagania dotyczące oprogramowania

2.5.1 ➡ Aplikacje mogą używać tylko publicznych interfejsów API i działać w aktualnie oferowanym systemie operacyjnym. Dowiedz się więcej o [publicznych interfejsach API](#). Dbaj o aktualność aplikacji i stopniowo wycofuj wszystkie przestarzałe funkcje, architektury lub technologie, które nie będą już obsługiwane w przyszłych wersjach systemu operacyjnego. Aplikacje powinny używać interfejsów API i architektur zgodnie z ich przeznaczeniem oraz wskazywać tę integrację w opisie aplikacji. Na przykład architektura HomeKit powinna zapewniać usługi automatyzacji domu, a architektura HealthKit powinna być używana do celów związanych ze zdrowiem i sprawnością fizyczną oraz integrować się z aplikacją Zdrowie.

2.5.2 ➡ Aplikacje powinny być samodzielne w swoich pakietach i nie mogą odczytywać ani zapisywać danych poza wyznaczonym obszarem kontenera. Nie mogą też pobierać, instalować ani wykonywać kodu, który wprowadza lub zmienia cechy bądź funkcjonalność aplikacji, w tym innych aplikacji. Aplikacje edukacyjne przeznaczone do nauczania, programowania lub testowania kodu wykonywalnego przez uczniów mogą, w ograniczonych przypadkach, pobierać kod pod warunkiem, że nie zostanie on użyty do innych celów. W takich aplikacjach kod źródłowy udostępniany przez aplikację musi być w pełni widoczny i edytowalny przez użytkownika.

2.5.3 ➡ Aplikacje przesyłające wirusy, pliki, kod komputerowy lub programy, które mogą uszkodzić lub zakłócić normalne działanie systemu operacyjnego i/lub funkcji sprzętowych, w tym powiadomienia push i Game Center, będą odrzucane. Rażąco naruszające i powtarzające się działania spowodują usunięcie z programu Apple Developer Program.

2.5.4 ➡ Aplikacje wielozadaniowe mogą korzystać z usług w tle tylko zgodnie z ich przeznaczeniem: VoIP, odtwarzanie dźwięku, lokalizacja, wykonywanie zadań, lokalne powiadomienia itp.

2.5.5 Aplikacje muszą być w pełni funkcjonalne w sieciach obsługujących wyłącznie protokół IPv6.

2.5.6 ➡ Aplikacje, które przeglądają Internet, muszą korzystać z odpowiedniej architektury WebKit i kodu JavaScript WebKit. Użytkownik może ubiegać się o prawo do wykorzystania alternatywnego silnika przeglądarki internetowej w swojej aplikacji. [Dowiedz się więcej o tych uprawnieniach](#).

2.5.7 Celowo pominięte.

2.5.8 Aplikacje, które tworzą alternatywne środowiska biurka/ekranu początkowego lub symulują działanie widżetów obejmujących wiele aplikacji, będą odrzucane.

2.5.9 ➡ Aplikacje, które zmieniają lub wyłączają funkcje standardowych przełączników, takich jak przyciski zwiększania/zmniejszania głośności i przełącznik dzwonka/wyciszenia, lub inne natywne elementy lub sposoby działania interfejsu użytkownika, będą odrzucane. Na przykład aplikacje nie powinny blokować łączy do innych aplikacji lub innych funkcji, które według oczekiwań użytkowników mają działać w określony sposób.

2.5.10 Nie należy zgłaszać aplikacji z pustymi banerami reklamowymi ani reklamami testowymi.

2.5.11 ➡ SiriKit i Skróty

(i) Aplikacje integrujące SiriKit i Skróty powinny rejestrować tylko takie intencje, które mogą obsłużyć bez wsparcia dodatkowej aplikacji i których użytkownicy oczekiwaliby od podanej funkcjonalności. Na przykład jeśli aplikacja jest aplikacją do planowania posiłków, nie powinna zawierać intencji rozpoczęcia treningu, nawet jeśli jest zintegrowana z aplikacją fitnessową.

(ii) Upewnij się, że słownictwo i frazy w pliku plist dotyczą Twojej aplikacji i funkcjonalności Siri w zakresie intencji, dla których aplikacja została zarejestrowana. Aliasy muszą odnosić się bezpośrednio do Twojej aplikacji lub nazwy firmy i nie mogą być terminami ogólnymi ani zawierać nazw aplikacji lub usług stron trzecich.

(iii) Prośby do Siri lub skróty powinny być realizowane w najbardziej bezpośredni sposób i nie należy wstawiać reklam ani innych elementów marketingowych między prośbą a jej realizacją. Prośba o ujednoznacznienie jest dozwolona tylko wtedy, gdy jest to wymagane do wykonania zadania (np. prośenie użytkownika o określenie konkretnego rodzaju treningu).

2.5.12 ➡ Aplikacje korzystające z CallKit lub zawierające rozszerzenie SMS Fraud Extension powinny blokować tylko numery telefonów potwierdzone jako spam. Aplikacje, które oferują funkcje blokowania połączeń, wiadomości SMS i MMS lub identyfikacji spamu, muszą wyraźnie określać te funkcje w swoich tekstach marketingowych i wyjaśniać kryteria, według których tworzone są listy zablokowanych i spamu. Nie możesz wykorzystywać danych dostępnych za pośrednictwem tych narzędzi w żadnym celu, który nie jest bezpośrednio związany z obsługą lub ulepszaniem Twojej aplikacji lub rozszerzenia (np. nie możesz używać, udostępniać ani sprzedawać ich do celów śledzenia, tworzenia profili użytkowników itp.).

2.5.13 ➡ Aplikacje korzystające z rozpoznawania twarzy do uwierzytelniania konta muszą w miarę możliwości używać technologii [LocalAuthentication](#) (a nie ARKit lub innej technologii rozpoznawania twarzy) oraz muszą używać alternatywnej metody uwierzytelniania dla użytkowników poniżej 13. roku życia.

2.5.14 ➡ Aplikacje muszą wymagać wyraźnej zgody użytkownika i zapewniać wyraźne wizualne i/lub dźwiękowe wskazanie podczas nagrywania, rejestrowania lub innego zapisu aktywności użytkownika. Obejmuje to wszelkie użycie aparatu urządzenia, mikrofonu, nagrań ekranu lub innych danych wprowadzanych przez użytkownika.

2.5.15 Aplikacje umożliwiające użytkownikom przeglądanie i wybieranie plików powinny zawierać elementy z aplikacji Pliki oraz folderu dokumentów iCloud użytkownika.

2.5.16 ➡ Wycinki aplikacji, widżety, rozszerzenia i powiadomienia powinny być powiązane z treścią i funkcjonalnością aplikacji.

(a) Ponadto wszystkie cechy i funkcje wycinka aplikacji muszą być zawarte w głównym pliku binarnym aplikacji. Wycinki aplikacji nie mogą zawierać reklam.

2.5.17 ➡ Aplikacje obsługujące standard Matter muszą korzystać z architektury wsparcia Apple, aby zainicjować łączenie w parę. Ponadto jeśli zdecydujesz się użyć w swojej aplikacji dowolnego komponentu oprogramowania Matter innego niż pakiet Matter SDK dostarczony przez Apple, komponent oprogramowania musi mieć certyfikat organizacji [Connectivity Standards Alliance](#) dla platformy, na której działa.

2.5.18 ➡ Reklamy wyświetlane powinny być ograniczone do głównego pliku binarnego aplikacji i nie powinny być uwzględniane w rozszerzeniach, wycinkach aplikacji, widżetach, powiadomieniach, klawiaturach, aplikacjach dla systemu watchOS itp. Reklamy wyświetlane w aplikacji muszą być odpowiednie dla klasyfikacji wiekowej aplikacji, umożliwiać użytkownikowi wyświetlenie wszystkich informacji użytych do skierowania do niego tej reklamy (bez konieczności opuszczania aplikacji przez użytkownika) i nie mogą angażować się w reklamy kierowane lub behawioralne oparte na wrażliwych danych użytkownika, takich jak dane dotyczące zdrowia / dane medyczne (np. z interfejsów API HealthKit), dane szkolne i klasowe (np. z ClassKit) lub dane dotyczące dzieci (np. z aplikacji z kategorii Dzieci w App Store) itp. Reklamy pełnoekranowe lub reklamy, które zakłócają lub blokują możliwość korzystania z aplikacji przez użytkownika, muszą wyraźnie wskazywać, że są reklamą, nie mogą manipulować ani nakłaniać użytkowników do ich kliknięcia oraz muszą zawierać łatwo dostępne i widoczne przyciski zamykania/pomijania, wystarczająco duże, aby użytkownicy mogli z łatwością odrzucić reklamę. Aplikacje zawierające reklamy muszą też umożliwiać użytkownikom zgłaszanie wszelkich nieodpowiednich lub nieodpowiednich dla dzieci reklam.

3. Model biznesowy

W App Store istnieje wiele sposobów zarabiania na aplikacji. Jeśli Twój model biznesowy nie jest oczywisty, koniecznie wyjaśnij go w metadanych aplikacji oraz w uwagach do zespołu App Review. Jeśli nie będziemy w stanie zrozumieć, jak działa Twoja aplikacja, lub zakupy w aplikacji nie są od razu

oczywiste, opóźni to weryfikację aplikacji i może spowodować jej odrzucenie. Wprawdzie ceny zależą od Ciebie, ale nie będziemy dystrybuować aplikacji ani przedmiotów do zakupów w aplikacji, które są jawnym zdzierstwem. Będziemy odrzucać drogie aplikacje, które próbują oszukać użytkowników irracjonalnie wysokimi cenami.

Jeżeli stwierdzimy, że próbujesz manipulować weryfikacjami, zawyżać swoje pozycje w rankingach za pomocą płatnych, motywowanych, filtrowanych lub fałszywych opinii albo angażować w takie działania w swoim imieniu strony trzecie, podejmiemy kroki w celu zachowania integralności App Store, które mogą obejmować wykluczenie Cię z programu Apple Developer Program.

3.1 Płatności

3.1.1 Zakup w aplikacji

- Jeśli chcesz odblokować cechy lub funkcje w swojej aplikacji (na przykład: subskrypcje, waluty w grze, poziomy gry, dostęp do treści premium lub odblokowanie pełnej wersji), musisz skorzystać z opcji zakupu w aplikacji. Aplikacje nie mogą korzystać z własnych mechanizmów do odblokowywania treści lub funkcji, takich jak klucze licencyjne, znaczniki rzeczywistości rozszerzonej, kody QR, kryptowaluty i portfele kryptowalut itp.
- Aplikacje mogą korzystać z waluty zakupów w aplikacji, aby umożliwić klientom przekazanie „napiwku” deweloperowi lub dostawcom treści cyfrowych w aplikacji.
- Wszelkie kredyty lub waluty w grze zakupione poprzez zakup w aplikacji nie mogą stracić ważności i musisz mieć mechanizm odtwarzania dla wszystkich możliwych do odtworzenia zakupów w aplikacji.
- Aplikacje mogą umożliwiać wręczanie innym osobom przedmiotów, które kwalifikują się do zakupu w aplikacji. Takie prezenty mogą zostać zwrócone tylko pierwotnemu nabywcy i nie podlegają wymianie.
- Aplikacje dystrybuowane za pośrednictwem Mac App Store mogą zawierać wtyczki lub rozszerzenia, które działają dzięki mechanizmom innym niż App Store.
- Aplikacje oferujące „skrzynki z łupami” lub inne mechanizmy zapewniające losowe wirtualne przedmioty do zakupu muszą ujawniać szanse otrzymania każdego rodzaju przedmiotu przed zakupem.
- Cyfrowe karty podarunkowe, certyfikaty, bony i kupony, które można wymienić na cyfrowe towary lub usługi, mogą być sprzedawane w aplikacji tylko za pomocą zakupów w aplikacji. Fizyczne karty podarunkowe sprzedawane w aplikacji, a następnie wysyłane pocztą do klientów, mogą korzystać z metod płatności innych niż zakupy w aplikacji.
- Aplikacje nieobjęte subskrypcją mogą oferować bezpłatny czasowy okres próbny przed przedstawieniem opcji pełnego odblokowania przez skonfigurowanie nieużywalnego zakupu w aplikacji na poziomie ceny 0, który jest zgodny z konwencją nazewnictwa: „XX-dniowy okres próbny”. Przed rozpoczęciem okresu próbnego aplikacja musi jasno określić czas jego trwania oraz

treści lub usługi, które nie będą już dostępne po zakończeniu okresu próbnego, a także wszelkie dodatkowe opłaty, które użytkownik będzie musiał ponieść, aby uzyskać pełną funkcjonalność. Dowiedz się więcej o zarządzaniu dostępem do treści i czasie trwania okresu próbnego w dokumentach dotyczących [weryfikacji odbioru](#) oraz [sprawdzania urządzenia](#).

- Aplikacje mogą wykorzystywać zakupy w aplikacji do sprzedawania usług związanych z niezamiennymi tokenami (NFT), takich jak mintowanie, wystawianie i transfer. Aplikacje mogą umożliwiać użytkownikom przeglądanie ich własnych NFT, pod warunkiem, że posiadanie NFT nie powoduje odblokowania cech lub funkcji aplikacji. Aplikacje mogą umożliwiać użytkownikom przeglądanie kolekcji NFT będących własnością innych osób, pod warunkiem, że aplikacje nie zawierają przycisków, łączy zewnętrznych ani innych wezwań do działania, które kierują klientów do mechanizmów zakupu innych niż zakup w aplikacji.

3.1.1(a) Łącze do innych metod zakupu

Deweloperzy mogą ubiegać się o uprawnienie do udostępnienia w swojej aplikacji łącza do witryny internetowej, której deweloper jest właścicielem lub za którą odpowiada, w celu dokonania zakupu takich rzeczy. Dowiedz się więcej o [uprawnieniu](#). Zgodnie z umową dotyczącą uprawnienia, łącze może informować użytkowników o tym, gdzie i jak mogą kupić te rzeczy w aplikacji, oraz o fakcie, że takie rzeczy mogą być dostępne za stosunkowo niższą cenę. Korzystanie z tego uprawnienia jest ograniczone tylko do App Store w systemie iOS lub iPadOS na witrynie sklepowej w Stanach Zjednoczonych. Na wszystkich innych witrynach sklepowych aplikacje i ich metadane nie mogą zawierać przycisków, łączy zewnętrznych ani innych wezwań do działania, które kierują klientów do mechanizmów zakupu innych niż zakup w aplikacji.

Jeśli Twoja aplikacja będzie stosować praktyki marketingowe, które wprowadzają w błąd, lub dokonywać oszustw, w tym związanych z uprawnieniem, zostanie ona usunięta z App Store i może to skutkować usunięciem Cię z programu Apple Developer Program.

3.1.2 Subskrypcje

Aplikacje mogą oferować automatycznie odnawiane subskrypcje zakupów w aplikacji, niezależnie od kategorii w App Store. Dodając do aplikacji automatycznie odnawiane subskrypcje, postępuj zgodnie z poniższymi wskazówkami.

3.1.2(a) Dopuszczalne zastosowania

Jeśli oferujesz automatycznie odnawianą subskrypcję, musisz zapewnić stałą wartość dla klienta, a okres subskrypcji musi trwać co najmniej siedem dni i być dostępny na wszystkich urządzeniach użytkownika. Lista ta nie jest wyczerpująca, ale odpowiednie subskrypcje to na przykład: nowe poziomy gry, treści epizodyczne, obsługa wielu graczy, aplikacje oferujące stałe, istotne uaktualnienia, dostęp do dużych kolekcji lub stale uaktualnianych treści multimedialnych, oprogramowanie jako usługa („SAAS”) i obsługa chmury. Ponadto:

- Subskrypcje mogą być oferowane wraz z ofertami à la carte (np. możesz oferować subskrypcję całej biblioteki filmów, a także zakup lub wypożyczenie pojedynczego filmu).

- Możesz oferować jedną subskrypcję wspólną dla Twoich aplikacji i usług.
- Gry oferowane w ramach subskrypcji usługi przesyłania strumieniowego mogą oferować jedną subskrypcję, która jest współdzielona przez aplikacje i usługi stron trzecich, muszą one jednak być pobierane bezpośrednio z App Store, muszą być zaprojektowane tak, aby uniknąć podwójnej płatności przez subskrybenta, i nie powinny być niekorzystne dla klientów niebędących subskrybentami.
- Subskrypcje muszą działać na wszystkich urządzeniach użytkownika, na których jest dostępna aplikacja. Dowiedz się więcej o [udostępnianiu subskrypcji w swoich aplikacjach](#).
- Aplikacje nie mogą zmuszać użytkowników do oceniania aplikacji, recenzowania aplikacji, pobierania innych aplikacji ani wykonywania innych podobnych działań w celu uzyskania dostępu do funkcji, treści lub korzystania z aplikacji.
- Podobnie jak w przypadku wszystkich aplikacji, aplikacje oferujące subskrypcje powinny umożliwiać użytkownikowi uzyskanie tego, za co zapłacił, bez wykonywania dodatkowych zadań, takich jak publikowanie w mediach społecznościowych, przesyłanie kontaktów, logowanie się w aplikacji określoną liczbę razy itp.
- Subskrypcje mogą obejmować zużywalne punkty kredytowe, klejnoty, waluty w grze itp. Możesz też oferować subskrypcje, które obejmują dostęp do towarów zużywalnych po obniżonej cenie (np. członkostwo płatynowe, które udostępnia pakiety klejnotów po obniżonej cenie).
- W przypadku zmiany modelu biznesowego już istniejącej aplikacji na oparty na subskrypcji nie należy odbierać podstawowej funkcjonalności, za którą dotychczasowi użytkownicy już zapłacili. Na przykład klienci, którzy już wykupili opcję odblokowania pełnej wersji gry, powinni nadal mieć możliwość korzystania z pełnej wersji gry po wprowadzeniu modelu subskrypcji dla nowych klientów.
- Aplikacje z automatycznie odnawianą subskrypcją mogą oferować klientom bezpłatny okres próbny przez podanie odpowiednich informacji określonych w App Store Connect. [Dowiedz się więcej o oferowaniu subskrypcji](#).
- Aplikacje próbujące oszukać użytkowników będą usuwane z App Store. Obejmuje to aplikacje, które próbują nakłonić użytkowników do zakupu subskrypcji pod fałszywym pretekstem lub angażują się w praktyki polegające na oszustwie lub przynęcie. Aplikacje te zostaną usunięte z App Store i może to skutkować usunięciem Cię z programu Apple Developer Program.
- Aplikacje operatora komórkowego mogą obejmować automatycznie odnawiane subskrypcje muzyki i wideo w pakietach z nowymi planami danych komórkowych, za uprzednią zgodą Apple. Inne automatycznie odnawiane subskrypcje mogą być również zawarte w pakietach przy zakupie z nowymi planami danych komórkowych, po uprzednim zatwierdzeniu przez Apple, jeśli aplikacje operatora komórkowego obsługują zakupy w aplikacji dla użytkowników. Takie subskrypcje nie mogą obejmować dostępu do przedmiotów zużywalnych ani zniżek na nie i muszą zakończyć się równocześnie z planem transmisji danych komórkowych.

3.1.2(b) Podwyższanie i obniżanie poziomu subskrypcji

Użytkownicy powinni mieć możliwość bezproblemowego podwyższania/obniżania poziomu subskrypcji i nie powinni być w stanie przypadkowo zasubskrybować wielu odmian tej samej rzeczy. Zapoznaj się z [najlepszymi sposobami postępowania](#) na temat zarządzania opcjami podwyższania i obniżania poziomu subskrypcji.

3.1.2(c) Informacje o subskrypcji

Przed poproszeniem klienta o wykupienie subskrypcji należy jasno opisać, co użytkownik otrzyma za tę cenę. Ile rozwiązań problemów miesięcznie? Ile miejsca w chmurze? Jaki rodzaj dostępu do Twojej usługi? Upewnij się, że jasno przedstawiasz wymagania opisane w [Załączniku nr 2 Umowy licencyjnej programu Apple Developer Program](#).

3.1.3 Inne metody zakupu

Następujące aplikacje mogą korzystać z innych metod zakupu niż zakup w aplikacji. Aplikacje wymienione w tej sekcji nie mogą w ramach aplikacji zachęcać użytkowników do korzystania z innej metody zakupu niż zakup w aplikacji, z wyjątkiem przypadków opisanych w punkcie 3.1.3(a). Deweloperzy mogą wysyłać komunikaty poza aplikacją do swoich użytkowników o metodach zakupu innych niż zakup w aplikacji.

3.1.3(a) Aplikacje czytników

Aplikacje mogą umożliwiać użytkownikowi dostęp do wcześniej zakupionych treści lub subskrypcji treści (w szczególności: czasopism, gazet, książek, materiałów audio, muzyki i wideo). Aplikacje czytników mogą oferować tworzenie kont dla poziomów bezpłatnych i funkcje zarządzania kontami dla dotychczasowych klientów. Deweloperzy aplikacji czytników mogą ubiegać się o uprawnienie do korzystania z zewnętrznego łącza, aby udostępnić w swoich aplikacjach łącze informacyjne do witryny internetowej, której deweloper jest właścicielem lub za którą odpowiada, w celu utworzenia konta lub zarządzania nim. Dowiedz się więcej o [uprawnieniu do korzystania z łącza zewnętrznego](#).

3.1.3(b) Usługi wieloplatformowe

Aplikacje działające na wielu platformach mogą umożliwiać użytkownikom dostęp do treści, subskrypcji lub funkcji, które nabyli w Twojej aplikacji na innych platformach lub w Twojej witrynie internetowej, w tym do przedmiotów zużywalnych w grach wieloplatformowych, pod warunkiem, że przedmioty te są również dostępne jako [zakupy w aplikacji](#).

3.1.3(c) Usługi korporacyjne

Jeśli aplikacja jest sprzedawana bezpośrednio organizacjom lub grupom dla ich pracowników lub uczniów (na przykład profesjonalne bazy danych i narzędzia do zarządzania klasą), możesz zezwolić użytkownikom korporacyjnym na dostęp do wcześniej zakupionych treści lub subskrypcji. Sprzedaż konsumencka, indywidualna lub rodzinna musi korzystać z zakupów w aplikacji.

3.1.3(d) Usługi bezpośrednie

Jeśli aplikacja umożliwia zakup usług w czasie rzeczywistym między dwiema osobami fizycznymi (na przykład korepetycji z uczniami, konsultacji lekarskich, wycieczek po nieruchomościach lub treningów fitness), do odbierania tych płatności możesz korzystać z metod zakupu innych niż zakup w aplikacji. Usługi w czasie rzeczywistym „jeden do kilku” i „jeden do wielu” muszą korzystać z zakupów w aplikacji.

3.1.3(e) Towary i usługi poza aplikacją

Jeśli aplikacja umożliwia kupowanie fizycznych towarów lub usług, które zostaną skonsumowane poza aplikacją, do odbierania tych płatności musisz użyć metod zakupu innych niż zakup w aplikacji, takich jak Apple Pay lub tradycyjna karta kredytowa.

3.1.3(f) Bezpłatne samodzielne aplikacje

Bezpłatne aplikacje działające jako samodzielny dodatek do płatnych narzędzi internetowych (np. VOIP, miejsce w chmurze, usługi e-mail, hosting www) nie muszą korzystać z zakupów w aplikacji, pod warunkiem, że nie ma żadnych zakupów wewnątrz aplikacji ani wezwań do działania w celu zakupu poza aplikacją.

3.1.3(g) Aplikacje do zarządzania reklamami

Aplikacje, których jedynym celem jest umożliwienie reklamodawcom (osobom lub firmom reklamującym produkt, usługę lub wydarzenie) kupowanie kampanii reklamowych w różnych rodzajach mediów (telewizja, reklamy zewnętrzne, strony internetowe, aplikacje itp.) i zarządzanie nimi, nie wymagają zakupów w aplikacji. Te aplikacje są przeznaczone do zarządzania kampaniami i same nie wyświetlają reklam. Cyfrowe zakupy treści, które są oglądane lub zużywane w aplikacji, w tym kupowanie reklam do wyświetlenia w tej samej aplikacji (np. sprzedaż „wzmocniaczy” dla postów w aplikacji społecznościowej), muszą odbywać się w ramach zakupów w aplikacji.

3.1.4 Treści specyficzne dla sprzętu

W pewnych okolicznościach, na przykład gdy działanie funkcji zależy od określonego sprzętu, aplikacja może odblokować tę funkcję bez korzystania z zakupu w aplikacji (np. aplikacja astronomiczna, która dodaje funkcje po zsynchronizowaniu z teleskopem). Funkcje aplikacji, które działają w połączeniu z zatwierdzonym produktem fizycznym (takim jak zabawka) na zasadzie opcjonalnej, mogą odblokowywać funkcje bez korzystania z zakupów w aplikacji, pod warunkiem, że opcja zakupu w aplikacji jest również dostępna. Nie możesz jednak wymagać od użytkowników zakupu niepowiązanych produktów ani angażowania się w działania reklamowe lub marketingowe w celu odblokowania funkcji aplikacji.

3.1.5 Kryptowaluty

(i) Portfele: aplikacje mogą ułatwiać przechowywanie wirtualnej waluty, pod warunkiem, że są oferowane przez deweloperów zarejestrowanych jako organizacja.

(ii) Wydobywanie: aplikacje nie mogą wydobywać kryptowalut, chyba że przetwarzanie odbywa się poza urządzeniem (np. wydobywanie w chmurze).

(iii) Giełdy: aplikacje mogą ułatwiać transakcje lub transmisje kryptowalut na zatwierdzonej giełdzie, pod warunkiem, że są one oferowane wyłącznie w krajach lub regionach, w których aplikacja posiada odpowiednie licencje i pozwolenia na świadczenie wymiany kryptowalut.

(iv) Pierwsze oferty monet: aplikacje ułatwiające pierwsze oferty monet („ICO”), handel kontraktami terminowymi na kryptowaluty i inne kryptowaluty lub quasi-papiery wartościowe muszą pochodzić od uznanych banków, firm papierów wartościowych, sprzedawców kontraktów terminowych („FCM”) lub innych zatwierdzonych instytucji finansowych i muszą przestrzegać wszystkich obowiązujących przepisów prawa.

(v) Aplikacje kryptowalutowe nie mogą oferować waluty za wykonywanie zadań, takich jak pobieranie innych aplikacji, zachęcanie innych użytkowników do pobierania, umieszczanie postów w sieciach społecznościowych itp.

3.2 Inne kwestie związane z modelem biznesowym

Poniższe listy nie są wyczerpujące, a przesłane przez Ciebie zgłoszenie może spowodować zmianę lub uaktualnienie naszych zasad, ale oto kilka dodatkowych nakazów i zakazów, o których należy pamiętać:

3.2.1 Dopuszczalne

(i) Wyświetlanie własnych aplikacji do kupienia lub promocji w aplikacji, pod warunkiem, że aplikacja nie jest jedynie katalogiem Twoich aplikacji.

(ii) Wyświetlanie lub polecanie kolekcji aplikacji stron trzecich, które zostały zaprojektowane z myślą o określonej zatwierdzonej potrzebie (np. zarządzanie zdrowiem, lotnictwo, ułatwienia dostępu). Aplikacja powinna zapewniać solidne treści redakcyjne, aby nie sprawiała wrażenia zwykłej witryny sklepowej.

(iii) Wyłączanie dostępu do określonych zatwierdzonych treści do wypożyczenia (np. filmów, programów telewizyjnych, muzyki, książek) po upływie okresu wypożyczenia. Żadne inne przedmioty ani usługi nie mogą wygasać.

(iv) Karty z Portfela mogą służyć do dokonywania lub otrzymywania płatności, przesyłania ofert lub oferowania dokumentów identyfikacyjnych (takich jak bilety do kina, bony i wejściówki VIP). Inne zastosowania mogą skutkować odrzuceniem aplikacji i unieważnieniem danych logowania do Portfela.

(v) Aplikacje ubezpieczeniowe muszą być bezpłatne, zgodne z prawem w regionach dystrybucji i nie mogą korzystać z zakupów w aplikacji.

(vi) Zatwierdzone organizacje non profit mogą prowadzić zbiórkę pieniędzy bezpośrednio w swoich własnych aplikacjach lub w aplikacjach stron trzecich, pod warunkiem, że kampanie te są zgodne ze wszystkimi Wytycznymi Dotyczącymi Weryfikacji Aplikacji i obsługują Apple Pay. Aplikacje te muszą informować o sposobie wykorzystania środków, przestrzegać wszystkich wymaganych przepisów na szczeblu lokalnym i krajowym oraz zapewniać darczyńcom odpowiednie potwierdzenia do celów podatkowych. Dodatkowe informacje zostaną przekazane zespołowi App Review na żądanie. Platformy non profit, które łączą darczyńców z innymi organizacjami non profit, muszą mieć pewność, że każda organizacja non profit wymieniona w aplikacji przeszła przez proces zatwierdzania organizacji non profit. Dowiedz się więcej o uzyskiwaniu statusu [zatwierdzonej organizacji non profit](#).

(vii) Aplikacje mogą umożliwiać indywidualnym użytkownikom przekazanie upominku pieniężnego innej osobie bez korzystania z zakupów w aplikacji, pod warunkiem, że (a) upominek jest całkowicie opcjonalnym wyborem osoby obdarowującej oraz (b) 100 procent środków trafia do odbiorcy upominku. Jednak upominek, który w dowolnym momencie jest połączony lub powiązany z otrzymaniem treści lub usług cyfrowych, musi korzystać z zakupu w aplikacji.

(viii) Aplikacje służące do handlu finansowego, inwestowania lub zarządzania środkami pieniężnymi powinny być zgłaszane przez instytucję finansową świadczącą takie usługi.

3.2.2 Niedopuszczalne

(i) Stworzenie interfejsu do wyświetlania aplikacji, rozszerzeń lub wtyczek stron trzecich podobnych do App Store lub w formie kolekcji o charakterze ogólnym.

(ii) Celowo pominięte.

(iii) Sztuczne zwiększanie liczby wyświetleń lub kliknięć reklam, a także aplikacje, które są zaprojektowane głównie do wyświetlania reklam.

(iv) Zbieranie środków w aplikacji na cele charytatywne oraz zbiórki pieniędzy, chyba że jesteś zatwierdzoną organizacją non profit lub podmiotem dozwolonym w inny sposób na mocy punktu 3.2.1 (vi) powyżej. Aplikacje, które chcą zbierać pieniądze na takie cele, muszą być dostępne bezpłatnie w App Store i mogą zbierać środki tylko poza aplikacją, na przykład za pośrednictwem przeglądarki Safari lub wiadomości SMS.

(v) Arbitralne ograniczanie osób, które mogą korzystać z aplikacji, na przykład ze względu na lokalizację lub operatora.

(vi) Celowo pominięte.

(vii) Sztuczne manipulowanie widocznością, statusem lub pozycją użytkownika w innych usługach, chyba że jest to dozwolone w warunkach korzystania z danej usługi.

(viii) Aplikacje ułatwiające handel opcjami binarnymi nie są dozwolone w App Store. Rozważ zamiast tego aplikację internetową. Aplikacje ułatwiające handel kontraktami na różnice kursowe („CFD”) lub innymi instrumentami pochodnymi (np. FOREX) muszą posiadać odpowiednią licencję we wszystkich jurysdykcjach, w których dostępna jest usługa.

(ix) Aplikacje oferujące pożyczki osobiste muszą jasno i wyraźnie ujawniać wszystkie warunki pożyczki, w tym między innymi równoważną maksymalną roczną stopę procentową (APR) oraz termin płatności. Aplikacje nie mogą pobierać maksymalnej APR wyższej niż 36%, włączając w to koszty i opłaty, oraz nie mogą wymagać spłaty całości w ciągu 60 dni lub mniej.


4. Projekt

Klienci Apple cenią sobie produkty, które są proste, dopracowane, innowacyjne i łatwe w użyciu — i takie właśnie aplikacje chcemy widzieć w App Store. Wymyślenie świetnego projektu należy do Ciebie, ale poniżej przedstawiono minimalne standardy zatwierdzania w App Store. Pamiętaj też, że nawet po

zatwierdzeniu aplikacji należy ją uaktualniać, aby nadal działała i była atrakcyjna dla nowych oraz obecnych klientów. Aplikacje, które przestają działać lub oferują pogorszone doświadczenia, mogą zostać w każdej chwili usunięte z App Store.

4.1 Naśladownictwo

(a) Wprowadzaj w życie własne pomysły. Wiemy, że je masz, wystarczy je urzeczywistnić. Nie kopiuj zwyczajnie najnowszej popularnej aplikacji z App Store ani nie wprowadzaj drobnych zmian w nazwie lub interfejsie innej aplikacji i nie przedstawiaj jej jako własnej. Oprócz ryzyka roszczeń o naruszenie praw własności intelektualnej utrudnia to poruszanie się po App Store i po prostu nie jest uczciwe wobec innych deweloperów.

(b)  Przesyłanie aplikacji, które podszywają się pod inne aplikacje lub usługi, jest uważane za naruszenie Kodeksu postępowania programistów i może skutkować usunięciem z programu Apple Developer Program.

4.2 Minimalna funkcjonalność

Aplikacja powinna zawierać funkcje, treści i interfejs użytkownika, które sprawiają, że jest czymś więcej niż tylko stroną internetową w nowym opakowaniu. Jeśli Twoja aplikacja nie jest szczególnie użyteczna, niepowtarzalna lub nie działa w sposób charakterystyczny dla aplikacji, nie ma dla niej miejsca w App Store. Jeśli aplikacja nie zapewnia trwałej wartości rozrywkowej ani odpowiedniej użyteczności, może nie zostać zaakceptowana. Aplikacje będące jedynie piosenką lub filmem należy przysyłać do iTunes Store. Aplikacje będące jedynie książką lub przewodnikiem po grze należy przysyłać do Apple Books Store.

4.2.1 Aplikacje korzystające z ARKit powinny zapewniać bogate i zintegrowane środowisko rozszerzonej rzeczywistości. Samo upuszczenie modelu do widoku AR lub odtworzenie animacji nie wystarczy.

4.2.2 Poza katalogami, aplikacje nie powinny być przede wszystkim materiałami marketingowymi, reklamami, wycinkami witryny, agregatorami treści ani zbiorami łączy.

4.2.3

(i) Aplikacja powinna działać samodzielnie, bez konieczności instalowania innej aplikacji.

(ii) Jeśli aplikacja musi pobrać dodatkowe zasoby, aby mogła działać przy pierwszym uruchomieniu, musi ujawnić rozmiar pobieranego pliku i poinformować użytkowników, zanim to zrobi.

4.2.4 Celowo pominięte.

4.2.5 Celowo pominięte.

4.2.6 Aplikacje utworzone na podstawie komercyjnego szablonu lub usługi generowania aplikacji zostaną odrzucone, chyba że zostaną zgłoszone bezpośrednio przez dostawcę treści aplikacji. Usługi te nie powinny zgłaszać aplikacji w imieniu swoich klientów i powinny oferować narzędzia umożliwiające klientom tworzenie niestandardowych, innowacyjnych aplikacji zapewniających wyjątkowe doświadczenia. Inną

akceptowaną opcją dla dostawców szablonów jest utworzenie pojedynczego pliku binarnego do hostowania całej zawartości klienta w modelu zagregowanym lub modelu „selektora”, na przykład jako aplikację do wyszukiwania restauracji z oddzielnymi dostosowanymi wpisami lub stronami dla każdej restauracji klienta lub jako aplikację do obsługi wydarzeń z oddzielnymi wpisami dla każdego wydarzenia klienta.

4.2.7 Klienci Remote Desktop

Jeśli aplikacja typu Remote Desktop działa jako kopia lustrzana określonego oprogramowania lub usług, a nie jako ogólna kopia lustrzana urządzenia głównego, musi być zgodna z następującymi zasadami:

(a) Aplikacja może łączyć się wyłącznie z urządzeniem głównym będącym własnością użytkownika, czyli komputerem osobistym lub dedykowaną konsolą do gier należącymi do użytkownika, a zarówno urządzenie główne, jak i klient muszą być połączone w sieci lokalnej i sieci LAN.

(b) Wszelkie oprogramowanie lub usługi pojawiające się na kliencie są w pełni wykonywane na urządzeniu głównym, renderowane na ekranie urządzenia głównego i nie mogą korzystać z interfejsów API ani funkcji platformy poza tymi, które są wymagane do strumieniowania Remote Desktop.

(c) Wszystkie operacje tworzenia kont i zarządzania nimi muszą być inicjowane z urządzenia głównego.

(d) Interfejs użytkownika wyświetlany na kliencie nie przypomina widoku systemu iOS lub App Store, nie zapewnia interfejsu sklepu ani nie umożliwia przeglądania, wybierania lub kupowania oprogramowania, które nie jest własnością użytkownika ani nie jest przez niego licencjonowane. Dla jasności, transakcje odbywające się w ramach lustrzanego oprogramowania nie muszą korzystać z zakupów w aplikacji, pod warunkiem, że transakcje te są przetwarzane na urządzeniu głównym.

(e) Klienci typu thin client dla aplikacji chmurowych nie są odpowiedni dla App Store.

4.3 Spam

(a) ❌ Nie należy tworzyć wielu identyfikatorów pakietów dla tej samej aplikacji. Jeśli aplikacja ma różne wersje dla konkretnych lokalizacji, drużyn sportowych, uniwersytetów itp., rozważ przesłanie jednej aplikacji i udostępnienie jej wariantów za pomocą zakupu w aplikacji.

(b) Należy również unikać dokładania się do kategorii, która jest już zapełniona. W App Store jest już wystarczająco dużo aplikacji z pierdnięciami i beknęciami, latarek, wróżb, aplikacji randkowych, gier alkoholowych, aplikacji Kamasutry itp. Będziemy odrzucać te aplikacje, chyba że zapewnią unikalne, wysokiej jakości doświadczenie. Spamowanie sklepu może doprowadzić do usunięcia Cię z programu Apple Developer Program.

4.4 Rozszerzenia ❌

Aplikacje hostujące lub zawierające rozszerzenia muszą być zgodne z [Przewodnikiem programowania rozszerzeń aplikacji](#), [dokumentacją rozszerzeń aplikacji Safari](#) lub [dokumentacją rozszerzeń internetowych Safari](#) i powinny zawierać funkcje, takie jak ekrany pomocy i interfejsy ustawień tam, gdzie to możliwe. Należy jasno i dokładnie informować o tym, jakie rozszerzenia są dostępne, w tekście marketingowym aplikacji, a rozszerzenia nie mogą obejmować działań marketingowych, reklam ani zakupów w aplikacji.

4.4.1 ➡ Rozszerzenia klawiatury są objęte pewnymi dodatkowymi zasadami.

Rozszerzenia klawiatury muszą:

- Zapewniać funkcje wprowadzania danych z klawiatury (np. wpisywanych znaków);
- Być zgodne z wytycznymi dotyczącymi naklejek, jeśli klawiatura zawiera obrazy lub emoji;
- Zapewniać metodę przechodzenia do następnej klawiatury;
- Zachować funkcjonalność bez pełnego dostępu do sieci i nie wymagając pełnego dostępu;
- Zbierać informacje o aktywności użytkownika tylko w celu ulepszenia funkcjonalności rozszerzenia klawiatury użytkownika na urządzeniu z systemem iOS.

Rozszerzenia klawiatury nie mogą:

- Uruchamiać innych aplikacji oprócz Ustawień; ani
- Zmieniać przeznaczenia przycisków klawiatury na inne działania (np. przytrzymanie klawisza „return” w celu uruchomienia aparatu).

4.4.2 ➡ Rozszerzenia Safari muszą działać w aktualnej wersji Safari w odpowiednim systemie operacyjnym Apple. Nie mogą zakłócać działania elementów interfejsu użytkownika systemu ani przeglądarki Safari i nigdy nie mogą zawierać złośliwych ani wprowadzających w błąd treści lub kodu. Naruszenie tej zasady spowoduje usunięcie z programu Apple Developer Program. Rozszerzenia Safari nie powinny żądać dostępu do większej liczby stron internetowych, niż jest to absolutnie konieczne do ich działania.

4.4.3 Celowo pominięte.

4.5 ➡ Witryny i usługi Apple

4.5.1 ➡ Aplikacje mogą korzystać z zatwierdzonych kanałów Apple RSS, takich jak kanał RSS iTunes Store, ale nie mogą pobierać żadnych informacji z witryn Apple (np. apple.com, iTunes Store, App Store, App Store Connect, portal dla deweloperów itp.) ani tworzyć rankingów na podstawie tych informacji.

4.5.2 ➡ Apple Music

(i) MusicKit w systemie iOS umożliwia użytkownikom odtwarzanie katalogu Apple Music i lokalnej biblioteki muzycznej z poziomu aplikacji i gier. Gdy użytkownik udzieli pozwolenia na dostęp do swojego konta Apple Music, aplikacja może tworzyć playlisty, dodawać utwory do biblioteki i odtwarzać dowolne z milionów utworów z katalogu Apple Music. Użytkownicy muszą zainicjować odtwarzanie strumienia Apple Music i mieć możliwość nawigacji przy użyciu standardowych elementów sterujących multimediami, takich jak „odtwórz”, „wstrzymaj” i „pomiń”. Ponadto aplikacja nie może wymagać płatności ani pośrednio zarabiać na dostępie do usługi Apple Music (np. poprzez zakup w aplikacji, reklamę, żądanie informacji o użytkowniku itp.). Nie pobieraj, nie przesyłaj ani nie

udostępniaj plików muzycznych pochodzących z interfejsów API MusicKit, z wyjątkiem przypadków wyraźnie dozwolonych w dokumentacji [MusicKit](#).

(ii) Korzystanie z interfejsów API MusicKit nie zastępuje zabezpieczenia licencji, które mogą być potrzebne do głębszej lub bardziej złożonej integracji muzyki. Na przykład, jeśli chcesz, aby aplikacja odtwarzała konkretny utwór w określonym momencie lub tworzyła pliki audio lub wideo, które można udostępniać w mediach społecznościowych, musisz skontaktować się bezpośrednio z właścicielami praw, aby uzyskać ich zgodę (np. prawa do synchronizacji i adaptacji) i zasoby. Okładki i inne metadane mogą być wykorzystywane wyłącznie w związku z odtwarzaniem muzyki lub playlistami (w tym zrzutami ekranu przedstawiającymi funkcjonalność aplikacji) i nie powinny być wykorzystywane w celach marketingowych ani reklamowych bez uzyskania specjalnego zezwolenia od posiadaczy praw. Podczas integracji usług Apple Music w aplikacji należy przestrzegać [wytycznych dotyczących tożsamości dla Apple Music](#).

(iii) Aplikacje, które uzyskują dostęp do danych użytkownika Apple Music, takich jak playlisty i ulubione, muszą wyraźnie informować o tym dostępie w tekście informującym o przeznaczeniu. Żadne zebrane dane nie mogą być udostępniane stronom trzecim w żadnym innym celu niż wspieranie lub ulepszanie aplikacji. Dane te nie mogą być wykorzystywane do identyfikacji użytkowników lub urzędzeń ani do kierowania reklam.

4.5.3 ❗ Nie używaj usług Apple, w tym Game Center, powiadomień push itp., do spamowania, wyłudzenia informacji lub wysyłania niechcianych wiadomości do klientów. Nie podejmuj prób odwrotnego wyszukiwania, śledzenia, powiązywania, kojarzenia, wydobywania, zbierania lub innego wykorzystywania identyfikatorów graczy, aliasów lub innych informacji uzyskanych za pośrednictwem Game Center, gdyż będzie to skutkowało usunięciem Cię z programu Apple Developer Program.

4.5.4 ❗ Powiadomienia push nie mogą być wymagane do działania aplikacji i nie powinny być używane do wysyłania wrażliwych informacji osobistych lub poufnych. Powiadomień push nie należy używać do celów promocyjnych lub marketingu bezpośredniego, chyba że klienci wyraźnie wyrazili zgodę na ich otrzymywanie za pośrednictwem języka zgody wyświetlanego w interfejsie użytkownika aplikacji, a Ty zapewniasz w swojej aplikacji metodę rezygnacji z otrzymywania takich wiadomości. Nadużywanie tych usług może spowodować odebranie uprawnień.

4.5.5 ❗ Identyfikatorów graczy z Game Center należy używać wyłącznie w sposób zatwierdzony przez warunki Game Center i nie należy ich wyświetlać w aplikacji ani stronom trzecim.

4.5.6 ❗ Aplikacje mogą używać znaków Unicode, które są renderowane jako emoji Apple w aplikacjach i ich metadanych. Emoji Apple nie mogą być używane na innych platformach ani osadzone bezpośrednio w plikach binarnych aplikacji.

4.6 Alternatywne ikony aplikacji ❗

Aplikacje mogą wyświetlać dostosowane ikony, na przykład w celu odzwierciedlenia preferencji drużyny sportowej, pod warunkiem, że każda zmiana jest inicjowana przez użytkownika, a aplikacja zawiera ustawienia umożliwiające przywrócenie oryginalnej ikony. Wszystkie warianty ikon muszą być powiązane z zawartością aplikacji, a zmiany powinny być spójne we wszystkich zasobach systemowych, tak aby ikony wyświetlane w Ustawieniach, Powiadomieniach itp. pasowały do nowej ikony.

4.7 Miniaplikacje, minigry, gry do strumieniowania, czatboty i wtyczki

Aplikacje mogą oferować określone oprogramowanie, które nie jest wbudowane w pliki binarne, w szczególności miniaplikacje, minigry, gry do strumieniowania, czatboty i wtyczki. Ponosisz odpowiedzialność za każde takie oprogramowanie oferowane w swojej aplikacji, w tym za zapewnienie, że takie oprogramowanie jest zgodne z niniejszymi Wytycznymi i wszystkimi obowiązującymi przepisami. Oprogramowanie niezgodne z co najmniej jedną wytyczną spowoduje odrzucenie aplikacji. Należy również upewnić się, że oprogramowanie jest zgodne z dodatkowymi zasadami określonymi w punktach 4.7.1 i 4.7.5. Te dodatkowe zasady są ważne dla zachowania doświadczeń, których oczekują klienci sklepu App Store, oraz dla zapewnienia bezpieczeństwa użytkowników.

4.7.1 Oprogramowanie oferowane w aplikacjach w myśl tej zasady musi:

- pozostawać zgodne ze wszystkimi wytycznymi dotyczącymi ochrony prywatności, w tym między innymi zasadami określonymi w Wytycznych 5.1 dotyczących gromadzenia, wykorzystywania i udostępniania danych oraz danych wrażliwych (takich jak dane zdrowotne i dane osobowe dzieci);
- uwzględniać metodę filtrowania niewłaściwych materiałów, mechanizm zgłaszania treści i niezwłoczne reagowanie na zastrzeżenia oraz możliwość blokowania użytkowników naruszających zasady; oraz
- wykorzystywać możliwość zakupów w aplikacji w celu oferowania cyfrowych towarów lub usług użytkownikom końcowym.

4.7.2 Twoja aplikacja nie może rozszerzać ani udostępniać interfejsów API platformy natywnej na oprogramowanie bez uprzedniej zgody Apple.

4.7.3 Twoja aplikacja nie może udostępniać danych ani uprawnień prywatności żadnemu indywidualnemu oprogramowaniu oferowanemu w aplikacji bez uzyskanej w każdym przypadku wyraźnej zgody użytkownika.

4.7.4 Należy przygotować spis oprogramowania i metadanych dostępnych w aplikacji. Musi on zawierać uniwersalne łącza prowadzące do całego oprogramowania oferowanego w aplikacji.

4.7.5 Twoja aplikacja musi udostępniać klasyfikację wiekową odpowiednią dla dostępnej w aplikacji treści o najwyższej klasyfikacji wiekowej.

4.8 Usługi logowania ↩

Aplikacje, które korzystają z usług logowania innych firm lub usług logowania się za pośrednictwem kont serwisów społecznościowych (takie jak Logowanie przez Facebooka, Logowanie przez Google, Zaloguj się za pomocą Twittera, Zaloguj się przez LinkedIn, Zaloguj się przez Amazon lub Logowanie WeChat) w celu skonfigurowania lub uwierzytelnienia głównego konta użytkownika w aplikacji, muszą również oferować inną usługę logowania jako równoważną opcję, która spełnia następujące kryteria:

- usługa logowania ogranicza gromadzenie danych do nazwy i adresu e-mail użytkownika;
- usługa logowania pozwala użytkownikom zachować prywatny adres e-mail podczas konfigurowania konta; oraz

- usługa logowania nie zbiera danych dotyczących interakcji z aplikacją w celach reklamowych bez zgody.

Główne konto użytkownika to konto, które zakłada on w Twojej aplikacji w celu identyfikacji, zalogowania się i uzyskania dostępu do funkcji oraz powiązanych usług.

Inna usługa logowania nie jest wymagana, jeśli:

- Aplikacja korzysta wyłącznie z własnych firmowych systemów konfiguracji konta i logowania.
- Twoja aplikacja to alternatywna platforma sprzedaży aplikacji lub aplikacja dystrybuowana za pośrednictwem alternatywnej platformy sprzedaży aplikacji, która korzysta z loginu właściwego dla danej platformy dla funkcji konta, pobierania i handlu.
- Aplikacja jest aplikacją edukacyjną, korporacyjną lub biznesową, która wymaga od użytkownika zalogowania się przy użyciu istniejącego konta edukacyjnego lub korporacyjnego.
- Aplikacja korzysta z rządowego lub wspieranego przez branżę systemu identyfikacji obywateli lub elektronicznego identyfikatora do uwierzytelniania użytkowników.
- Aplikacja jest aplikacją kliencką określonej usługi strony trzeciej, a użytkownicy muszą logować się bezpośrednio do swojej poczty, mediów społecznościowych lub innego konta strony trzeciej, aby uzyskać dostęp do swoich treści.

4.9 Apple Pay ↻

Aplikacje korzystające z usługi Apple Pay muszą dostarczyć użytkownikowi wszystkie istotne informacje dotyczące zakupu przed sprzedażą jakiegokolwiek towaru lub usługi i muszą prawidłowo używać elementów marki Apple Pay oraz elementów interfejsu użytkownika, zgodnie z opisem w artykułach Apple Pay Marketing Guidelines (Wytyczne marketingowe dotyczące usługi Apple Pay) i Human Interface Guidelines (Wytyczne dotyczące interfejsu użytkownika). Aplikacje korzystające z usługi Apple Pay do oferowania płatności cyklicznych muszą przedstawiać co najmniej następujące informacje:

- Długość okresu odnowienia oraz fakt, że będzie ono kontynuowane do momentu anulowania
- Co będzie zapewnione w każdym okresie
- Rzeczywiste opłaty, którymi zostanie obciążony klient
- Sposób anulowania

4.10 Zarabianie na wbudowanych funkcjach ↻

Nie możesz zarabiać na wbudowanych funkcjach zapewnianych przez sprzęt lub system operacyjny, takich jak Powiadomienia push, aparat lub żyroskop, ani na usługach i technologiach Apple, takich jak dostęp do usługi Apple Music, pamięć masowa iCloud lub interfejsy API funkcji Czas przed ekranem.

5. Informacje prawne ↩️

Aplikacje muszą być zgodne ze wszystkimi wymogami prawnymi w każdym miejscu, w którym są udostępniane (w razie wątpliwości należy skontaktować się z prawnikiem). Wiemy, że to skomplikowane, ale Twoim obowiązkiem jest zrozumienie i upewnienie się, że Twoja aplikacja jest zgodna ze wszystkimi lokalnymi przepisami, a nie tylko z poniższymi wytycznymi. Aplikacje, które nakłaniają lub zachęcają do zachowań przestępczych lub wyraźnie lekkomyślnych albo je promują, będą oczywiście odrzucane. W skrajnych przypadkach, takich jak aplikacje ułatwiające handel ludźmi i/lub wykorzystywanie dzieci, zostaną powiadomione odpowiednie władze.

5.1 Prywatność ↩️

Ochrona prywatności użytkowników jest sprawą nadrzędną w ekosystemie Apple. Przetwarzając dane osobowe, musisz zachować ostrożność, aby mieć pewność, że są przestrzegane [najlepsze sposoby postępowania dotyczące prywatności](#), obowiązujące przepisy prawa i warunki [umowy licencyjnej programu Apple Developer Program](#), o oczekiwaniach klientów nie wspominając. W szczególności:

5.1.1 Gromadzenie i przechowywanie danych ↩️

(i) Zasady ochrony prywatności: Wszystkie aplikacje muszą zawierać łącze do swoich zasad ochrony prywatności w polu metadanych App Store Connect oraz w aplikacji w łatwo dostępnym miejscu. Zasady ochrony prywatności muszą jasno i wyraźnie:

- Określać, jakie dane (jeśli w ogóle) zbiera aplikacja/usługa, w jaki sposób to robi i w jaki sposób je wykorzystuje.
- Potwierdzać, że każda strona trzecia, której aplikacja udostępnia dane użytkownika (zgodnie z niniejszymi wytycznymi) — na przykład narzędzia analityczne, sieci reklamowe i pakiety SDK innych firm, a także wszelkie podmioty nadrzędne, zależne lub inne podmioty powiązane, które będą miały dostęp do danych użytkownika — zapewni taką samą lub równą ochronę danych użytkownika, jak określono w zasadach ochrony prywatności aplikacji, i zgodnie z wymaganiami niniejszych wytycznych.
- Wyjaśniać zasady przechowywania/usuwania danych i opisywać, w jaki sposób użytkownik może odwołać zgodę i/lub zażądać usunięcia swoich danych.

(ii) Pozwolenie: Aplikacje, które zbierają dane użytkownika lub dane dotyczące użytkownika, muszą uzyskać zgodę użytkownika na ich zbieranie, nawet jeśli dane te są uważane za anonimowe w momencie ich zbierania lub bezpośrednio po ich zebraniu. Płatne funkcje nie mogą być uzależnione od udzielenia przez użytkownika dostępu do tych danych ani wymagać udzielenia takiego dostępu. Aplikacje muszą też zapewniać klientowi łatwo dostępną i zrozumiałą metodę wycofania zgody. Upewnij się, że teksty informujące o przeznaczeniu jasno i wyczerpująco opisują, w jaki sposób wykorzystujesz dane. Aplikacje, które gromadzą dane w uzasadnionym interesie bez zgody, opierając się na warunkach ogólnego rozporządzenia Unii Europejskiej o ochronie danych („RODO”) lub

podobnych przepisów, muszą przestrzegać wszystkich warunków tego prawa. Dowiedz się więcej na temat [proszenia o pozwolenie](#).

(iii) Minimalizacja danych: Aplikacje powinny żądać dostępu wyłącznie do danych istotnych dla głównej funkcjonalności aplikacji oraz powinny zbierać i wykorzystywać tylko te dane, które są niezbędne do wykonania danego zadania. Jeśli to możliwe, użyj selektora pozaprocesowego lub arkusza udostępniania, zamiast prosić o pełny dostęp do chronionych zasobów, takich jak Zdjęcia lub Kontakty.

(iv) Dostęp: Aplikacje muszą honorować ustawienia uprawnień użytkownika i nie mogą próbować manipulować, oszukiwać ani zmuszać użytkowników do wyrażenia zgody na niepotrzebny dostęp do danych. Na przykład aplikacje, które umożliwiają publikowanie zdjęć w sieciach społecznościowych, nie mogą również wymagać dostępu do mikrofonu przed zezwoleniem użytkownikowi na przesyłanie zdjęć. Jeśli to możliwe, należy zapewnić alternatywne rozwiązania dla użytkowników, którzy nie udzielają zgody. Na przykład jeśli użytkownik odmówi udostępnienia lokalizacji, zaoferuj mu możliwość ręcznego wprowadzenia adresu.

(v) Logowanie na konto: Jeśli aplikacja nie zawiera istotnych funkcji związanych z kontem, pozwól korzystać z niej bez logowania. Jeśli aplikacja obsługuje tworzenie konta, musisz również [oferować możliwość usunięcia konta w aplikacji](#). Aplikacje nie mogą swojego działania uzależniać od podania przez użytkowników danych osobowych, chyba że jest to bezpośrednio związane z podstawową funkcjonalnością aplikacji lub wymagane przez prawo. Jeśli podstawowa funkcjonalność aplikacji nie jest powiązana z konkretną siecią społecznościową (np. Facebook, WeChat, Weibo, X itp.), musisz zapewnić dostęp bez logowania lub za pomocą innego mechanizmu. Pobieranie podstawowych informacji profilowych, udostępnianie w sieciach społecznościowych lub zapraszanie znajomych do korzystania z aplikacji nie jest uważane za podstawową funkcjonalność aplikacji. Aplikacja musi również zawierać mechanizm odwoływania danych uwierzytelniania sieci społecznościowej i wyłączania dostępu do danych między aplikacją a siecią społecznościową z poziomu aplikacji. Aplikacja nie może przechowywać danych uwierzytelniania ani tokenów w sieciach społecznościowych poza urządzeniem i może używać takich danych uwierzytelniania lub tokenów wyłącznie do bezpośredniego łączenia się z siecią społecznościową z poziomu samej aplikacji podczas jej używania.

(vi) Deweloperzy używający swoich aplikacji do potajemnego odkrywania haseł lub innych prywatnych danych zostaną usunięci z programu Apple Developer Program.

(vii) Do wizualnego prezentowania informacji użytkownikom należy używać kontrolera SafariViewController. Kontroler nie może być ukryty ani zasłonięty przez inne widoki lub warstwy. Ponadto aplikacja nie może używać kontrolera SafariViewController do śledzenia użytkowników bez ich wiedzy i zgody.

(viii) Aplikacje gromadzące dane osobowe z jakiegokolwiek źródła, które nie pochodzą bezpośrednio od użytkownika, lub bez jego wyraźnej zgody, nawet z publicznych baz danych, nie są dozwolone w App Store ani na alternatywnych platformach sprzedaży aplikacji.

(ix) Aplikacje, które świadczą usługi w ściśle regulowanych dziedzinach (takich jak usługi bankowe i finansowe, opieka zdrowotna, hazard, legalne używanie konopi indyjskich i podróże lotnicze) lub które wymagają wrażliwych informacji o użytkowniku, powinny być zgłaszane przez podmiot prawny

świadczący usługi, a nie przez indywidualnego dewelopera. Aplikacje ułatwiające legalną sprzedaż konopi indyjskich muszą być ograniczone geograficznie do odpowiedniej jurysdykcji prawnej.

(x) Aplikacje mogą wymagać podania podstawowych danych kontaktowych (takich jak imię i nazwisko oraz adres e-mail), o ile żądanie jest dla użytkownika opcjonalne, funkcje i usługi nie są uzależnione od podania tych danych i jest to zgodne ze wszystkimi innymi postanowieniami niniejszych wytycznych, w tym z ograniczeniami dotyczącymi zbierania informacji od dzieci.

5.1.2 Wykorzystywanie i udostępnianie danych ↔

(i) O ile prawo nie stanowi inaczej, nie możesz wykorzystywać, przekazywać ani udostępniać danych osobowych innych osób bez uprzedniego uzyskania ich zgody. Musisz zapewnić dostęp do informacji o tym, jak i gdzie dane będą wykorzystywane. Dane zebrane z aplikacji mogą być udostępniane stronom trzecim wyłącznie w celu ulepszania aplikacji lub wyświetlania reklam (zgodnie z [umową licencyjną programu Apple Developer Program](#)). Aby śledzić aktywność użytkowników, musisz uzyskać od nich wyraźne pozwolenie za pośrednictwem interfejsów API App Tracking Transparency. Dowiedz się więcej o [śledzeniu](#). Aplikacja nie może wymagać od użytkowników włączenia funkcji systemowych (np. powiadomień push, usług lokalizacji, śledzenia) w celu uzyskania dostępu do funkcji, treści, korzystania z aplikacji bądź otrzymywania wynagrodzenia pieniężnego lub innego rodzaju, w tym między innymi kart upominkowych i kodów. Aplikacje, które udostępniają dane użytkownika bez jego zgody lub w sposób niezgodny z przepisami o ochronie danych osobowych, mogą zostać wycofane ze sprzedaży i skutkować usunięciem użytkownika z programu Apple Developer Program.

(ii) Dane zebrane w jednym celu nie mogą zostać wykorzystane w innym celu bez dodatkowej zgody, chyba że prawo wyraźnie na to zezwala.

(iii) Aplikacje nie powinny próbować potajemnie tworzyć profilu użytkownika na podstawie zebranych danych i nie mogą próbować, ułatwiać ani zachęcać innych do identyfikowania anonimowych użytkowników lub rekonstruowania profili użytkowników na podstawie danych zebranych z interfejsów API dostarczonych przez Apple lub jakichkolwiek innych danych, które według Ciebie zostały zebrane w sposób „zanonimizowany”, „zagregowany” lub w inny sposób uniemożliwiający identyfikację.

(iv) Nie wykorzystuj informacji z Kontaktów, Zdjęć ani innych interfejsów API, które uzyskują dostęp do danych użytkownika, do tworzenia bazy danych kontaktów na własny użytek lub do sprzedaży/dystrybucji wśród osób trzecich, a także nie zbieraj informacji o innych aplikacjach zainstalowanych na urządzeniu użytkownika w celach analitycznych lub reklamowych/marketingowych.

(v) Nie kontaktuj się z osobami przy użyciu informacji zebranych za pośrednictwem Kontaktów lub Zdjęć użytkownika, chyba że z wyraźnej inicjatywy tego użytkownika w sposób zindywidualizowany. Nie należy włączać opcji Wybierz wszystko ani domyślnie wybierać wszystkich kontaktów. Musisz przedstawić użytkownikowi jasny opis tego, jak wiadomość będzie wyglądać u odbiorcy, przed jej wysłaniem (np. co będzie zawierała wiadomość, kto będzie wyświetlany jako nadawca).

(vi) Dane zebrane z interfejsów API HomeKit, HealthKit, Clinical Health Records, MovementDisorder, ClassKit lub z narzędzi do mapowania głębi i/lub twarzy (np. ARKit, interfejsów API aplikacji Aparat lub interfejsów API aplikacji Zdjęcia) nie mogą być wykorzystywane do celów

marketingowych, reklamowych lub eksploracji danych na podstawie użytkowania, w tym przez strony trzecie. Dowiedz się więcej o najlepszych sposobach postępowania dotyczących interfejsu [CallKit](#), [HealthKit](#), [ClassKit](#) i [ARKit](#).

(vii) Aplikacje korzystające z usługi Apple Pay mogą udostępniać dane użytkownika uzyskane za pośrednictwem usługi Apple Pay stronom trzecim wyłącznie w celu ułatwienia lub usprawnienia dostarczania towarów i usług.

5.1.3 Zdrowie i badania w zakresie zdrowia ↗

Dane dotyczące zdrowia, sprawności fizycznej i dane medyczne są szczególnie wrażliwe, a aplikacje w tej przestrzeni mają dodatkowe zasady zapewniające ochronę prywatności klientów:

(i) Aplikacje nie mogą wykorzystywać ani ujawniać stronom trzecim danych zebranych w kontekście zdrowia, sprawności fizycznej i badań medycznych — w tym z interfejsów API Clinical Health Records, HealthKit, Motion and Fitness, MovementDisorder lub badań zdrowotnych na ludziach — do celów reklamowych, marketingowych lub innych celów eksploracji danych na podstawie użytkowania, innych niż poprawa zarządzania zdrowiem, lub do celów badań nad zdrowiem, a i wówczas tylko za zgodą. Aplikacje mogą jednak wykorzystywać dane dotyczące zdrowia lub sprawności fizycznej użytkownika w celu zapewnienia korzyści bezpośrednio temu użytkownikowi (np. obniżonej składki ubezpieczeniowej), pod warunkiem, że aplikacja zostanie zgłoszona przez podmiot zapewniający korzyść, a dane nie są udostępniane stronie trzeciej. Musisz ujawnić konkretne dane dotyczące zdrowia, które zbierasz z urządzenia.

(ii) Aplikacje nie mogą zapisywać fałszywych lub niedokładnych danych w HealthKit ani innych aplikacjach do badań medycznych lub zarządzania zdrowiem, a także nie mogą przechowywać osobistych informacji o stanie zdrowia w iCloud.

(iii) Aplikacje służące do prowadzenia badań naukowych związanych ze zdrowiem na ludziach muszą uzyskać zgodę uczestników lub, w przypadku osób niepełnoletnich, ich rodziców lub opiekunów. Taka zgoda musi zawierać (a) charakter, cel i czas trwania badań; (b) procedury, ryzyko i korzyści dla uczestnika; (c) informacje o poufności i sposobie postępowania z danymi (w tym o ich udostępnianiu osobom trzecim); (d) punkt kontaktowy w przypadku pytań uczestników; oraz (e) procedurę wycofania zgody.

(iv) Aplikacje służące do prowadzenia badań naukowych związanych ze zdrowiem na ludziach muszą uzyskać zgodę niezależnej komisji etycznej. Dowód takiej zgody należy przedstawić na żądanie.

5.1.4 Dzieci

(a) ↗ Z wielu powodów bardzo ważne jest zachowanie ostrożności przy przetwarzaniu danych osobowych dzieci, dlatego zachęcamy do dokładnego zapoznania się ze wszystkimi wymogami dotyczącymi przestrzegania przepisów takich jak ustawa o ochronie prywatności dzieci w Internecie („COPPA”), ogólne rozporządzenie Unii Europejskiej o ochronie danych („RODO”) oraz wszelkie inne obowiązujące przepisy lub prawa.

Aplikacje mogą prosić o podanie dat urodzenia i informacji kontaktowych rodziców tylko w celu zachowania zgodności z tymi przepisami, ale muszą zawierać pewne przydatne funkcje lub wartość rozrywkową niezależnie od wieku użytkownika.

Aplikacje przeznaczone głównie dla dzieci nie powinny zawierać narzędzi analitycznych ani reklam stron trzecich. Zapewnia to bezpieczniejsze doświadczenia dla dzieci.

(b) W niektórych przypadkach narzędzia analityczne i reklamy stron trzecich mogą być dozwolone pod warunkiem, że usługi są zgodne z warunkami określonymi w [Wytycznych 1.3](#).

Ponadto aplikacje z kategorii Dzieci lub aplikacje, które zbierają i przesyłają dane osobowe lub mają możliwość ich udostępniania (np. imienia i nazwiska, adresu, adresu e-mail, lokalizacji, zdjęć, filmów, rysunków, możliwości czatowania, innych danych osobowych lub trwałych identyfikatorów używanych w połączeniu z którymkolwiek z powyższych) od osoby niepełnoletniej muszą zawierać zasady ochrony prywatności i muszą być zgodne ze wszystkimi obowiązującymi przepisami dotyczącymi prywatności dzieci. Dla jasności, [wymóg dotyczący ochrony rodzicielskiej](#) w kategorii Dzieci nie jest tym samym, co uzyskanie zgody rodzicielskiej na gromadzenie danych osobowych na mocy tych przepisów o ochronie prywatności.

Przypominamy, że zgodnie z [Wytycznymi 2.3.8](#) używanie terminów takich jak „Dla dzieci” w metadanych aplikacji jest zarezerwowane wyłącznie dla kategorii Dzieci. Aplikacje spoza kategorii Dzieci nie mogą zawierać w nazwie aplikacji, podtytule, ikonie, zrzutach ekranu ani opisie żadnych terminów, które sugerują, że głównymi odbiorcami aplikacji są dzieci.

5.1.5 Usługi lokalizacji ↗

Korzystaj z usług lokalizacji w swojej aplikacji tylko wtedy, gdy jest to bezpośrednio związane z funkcjami i usługami świadczonymi przez aplikację. Interfejsy API oparte na lokalizacji nie powinny być wykorzystywane do świadczenia usług ratunkowych lub autonomicznej kontroli nad pojazdami, samolotami i innymi urządzeniami, z wyjątkiem małych urządzeń, takich jak lekkie drony i zabawki lub zdalnie sterowane systemy alarmowe samochodów itp. Przed zbieraniem, przesyłaniem lub używaniem danych dotyczących lokalizacji należy powiadomić o tym użytkownika i uzyskać jego zgodę. Jeśli aplikacja korzysta z usług lokalizacji, nie zapomnij wyjaśnić jej przeznaczenia. Zapoznaj się z [wytycznymi dotyczącymi interfejsu użytkownika](#), aby poznać najlepsze sposoby postępowania w tym zakresie.

5.2 Własność intelektualna

Upewnij się, że aplikacja zawiera tylko treści, które zostały utworzone przez Ciebie lub na które masz licencję. Aplikacja może zostać usunięta, jeśli przekroczysz tę granicę i użyjesz treści bez pozwolenia. Oczywiście oznacza to również, że aplikacja innej osoby może zostać usunięta, jeśli ta osoba „zapożyczyła” ją z Twojej pracy. Jeśli uważasz, że Twoja własność intelektualna została naruszona przez innego dewelopera w App Store, zgłoś roszczenie za pośrednictwem naszego [formularza internetowego](#). Przepisy różnią się w zależności od kraju i regionu, ale przynajmniej unikaj następujących typowych błędów:

5.2.1 Ogólnie: Nie używaj w swojej aplikacji bez pozwolenia materiałów chronionych, takich jak znaki towarowe, dzieła chronione prawem autorskim lub opatentowane pomysły, i nie umieszczaj w pakiecie aplikacji ani nazwie dewelopera wprowadzających w błąd, fałszywych lub naśladowczych oświadczeń, nazw lub metadanych. Aplikacje powinny być zgłaszane przez osobę fizyczną lub prawną, która jest właścicielem lub posiada licencję na własność intelektualną i inne odpowiednie prawa.

5.2.2 Witryny/usługi stron trzecich: Jeśli aplikacja korzysta z usługi strony trzeciej, uzyskuje do niej dostęp, zarabia na niej lub wyświetla treści z usługi strony trzeciej, upewnij się, że masz na to specjalne pozwolenie zgodnie z warunkami korzystania z usługi. Upoważnienie należy przedstawić na żądanie.

5.2.3 Pobieranie audio/wideo: Aplikacje nie powinny ułatwiać nielegalnego udostępniania plików ani umożliwiać zachowywania, konwertowania ani pobierania multimediów ze źródeł zewnętrznych (np. Apple Music, YouTube, SoundCloud, Vimeo itp.) bez wyraźnej zgody tych źródeł. Strumieniowe przesyłanie treści audio/wideo może również naruszać warunki użytkowania, dlatego należy to sprawdzić, zanim aplikacja uzyska dostęp do tych usług. Upoważnienie należy przedstawić na żądanie.

5.2.4 Referencje Apple:

(a) ❌ Nie sugeruj ani nie dawaj do zrozumienia, że Apple jest źródłem lub dostawcą aplikacji ani że Apple popiera jakiegokolwiek konkretne oświadczenie dotyczące jakości lub funkcjonalności.

(b) Jeśli aplikacja zostanie wybrana jako „Wybór redakcji”, Apple automatycznie zastosuje plaketkę.

5.2.5 Produkty Apple ❌ Nie twórz aplikacji, która wydaje się łudząco podobna do istniejącego produktu, interfejsu (np. Findera), aplikacji (takiej jak App Store, iTunes Store lub Wiadomości) lub motywu reklamowego Apple. Aplikacje i rozszerzenia, w tym klawiatury i pakiety naklejek stron trzecich, nie mogą zawierać emoji Apple. Muzyki z podglądów iTunes i Apple Music nie można używać do celów rozrywkowych (np. jako podkład muzyczny do kolażu zdjęć lub ścieżki dźwiękowej do gry) ani w żaden inny nieautoryzowany sposób. Jeśli udostępniasz podglądy muzyki z iTunes lub Apple Music, musisz wyświetlić łącze do odpowiedniej muzyki w iTunes lub Apple Music. Jeśli aplikacja wyświetla pierścienie aktywności, nie powinny one wizualizować danych W ruchu, Ćwiczenie lub Na nogach w sposób przypominający sterowanie aktywnością. Więcej informacji na temat korzystania z pierścieni aktywności zawiera dokument [Human Interface Guidelines](#) (Wytyczne dotyczące interfejsu użytkownika). Jeśli aplikacja wyświetla dane Pogody Apple, powinna być zgodna z wymaganiami atrybucji określonymi w [dokumentacji WeatherKit](#).

5.3 Gry, hazard i loterie

Gry, hazard i loterie mogą być trudne w zarządzaniu i zwykle stanowią jedną z najbardziej regulowanych ofert w App Store. Włączaj tę funkcjonalność tylko wtedy, gdy w pełni zweryfikujesz swoje zobowiązania prawne we wszystkich miejscach, w których udostępniasz aplikację, i akceptujesz fakt, że proces weryfikacji może potrwać dłużej. O czym należy pamiętać:

5.3.1 Loterie i konkursy muszą być sponsorowane przez dewelopera aplikacji.

5.3.2 Oficjalne zasady zakładów, konkursów i loterii fantowych muszą być prezentowane w aplikacji i jasno określać, że Apple nie jest sponsorem ani nie jest w żaden sposób zaangażowana w daną działalność.

5.3.3 Aplikacje nie mogą używać zakupów w aplikacji do kupowania środków lub waluty do użytku w połączeniu z jakimikolwiek gramami na prawdziwe pieniądze.

5.3.4 Aplikacje oferujące gry na prawdziwe pieniądze (np. zakłady sportowe, poker, gry w kasynie, wyścigi konne) lub loterie muszą posiadać niezbędne licencje i pozwolenia w miejscach, w których aplikacja jest używana, muszą być ograniczone geograficznie do tych miejsc i muszą być bezpłatne w App Store. Nielegalne pomoce hazardowe, w tym liczniki kart, są niedozwolone w App Store. Aplikacje loteryjne muszą obejmować zapłatę, los i wygraną.

5.4 Aplikacje VPN ↪

Aplikacje oferujące usługi VPN muszą korzystać z rozszerzenia [Interfejs API NEVPNManager](#) i mogą być oferowane tylko przez deweloperów zarejestrowanych jako organizacja. Musisz wyraźnie zadeklarować, jakie dane użytkownika będą zbierane oraz w jaki sposób będą one wykorzystywane, na ekranie aplikacji, zanim użytkownik podejmie jakiegokolwiek działania mające na celu zakup usługi lub korzystanie z niej w inny sposób. Aplikacje oferujące usługi VPN nie mogą sprzedawać, wykorzystywać ani ujawniać stronom trzecim żadnych danych w jakimkolwiek celu i muszą zobowiązać się do tego w swoich zasadach ochrony prywatności. Aplikacje VPN nie mogą naruszać lokalnego prawa, a jeśli zdecydujesz się udostępnić swoją aplikację VPN na terytorium, które wymaga licencji VPN, musisz podać informacje o licencji w polu uwag do weryfikacji aplikacji. Aplikacje do nadzoru rodzicielskiego, blokowania treści i zabezpieczeń pochodzące między innymi od zatwierdzonych dostawców mogą również korzystać z interfejsu API NEVPNManager. Aplikacje niezgodne z tymi wytycznymi zostaną usunięte z App Store, a możliwość ich instalacji za pośrednictwem alternatywnego kanału dystrybucji zostanie zablokowana; może to też skutkować usunięciem Cię z programu Apple Developer Program.

5.5 Zarządzanie urządzeniami mobilnymi ↪

Aplikacje do zarządzania urządzeniami mobilnymi, które oferują usługi zarządzania urządzeniami mobilnymi (MDM), muszą zamówić tę funkcję od Apple. Takie aplikacje mogą być oferowane wyłącznie przez przedsiębiorstwa komercyjne, instytucje edukacyjne lub agencje rządowe oraz, w ograniczonych przypadkach, przez firmy korzystające z MDM na potrzeby usług nadzoru rodzicielskiego lub bezpieczeństwa urządzeń. Musisz wyraźnie zadeklarować, jakie dane użytkownika będą zbierane oraz w jaki sposób będą one wykorzystywane, na ekranie aplikacji, zanim użytkownik podejmie jakiegokolwiek działania mające na celu zakup usługi lub korzystanie z niej w inny sposób. Aplikacje MDM nie mogą naruszać żadnych obowiązujących przepisów. Aplikacje oferujące usługi MDM nie mogą sprzedawać, wykorzystywać ani ujawniać stronom trzecim żadnych danych w jakimkolwiek celu i muszą zobowiązać się do tego w swoich zasadach ochrony prywatności. W niektórych przypadkach narzędzia analityczne stron trzecich mogą być dozwolone pod warunkiem, że usługi zbierają lub przesyłają tylko dane o działaniu aplikacji MDM dewelopera, a nie dane dotyczące użytkownika, urządzenia użytkownika lub innych aplikacji używanych na tym urządzeniu. Aplikacje oferujące profile konfiguracji również muszą spełniać te wymagania. Aplikacje niezgodne z tymi wytycznymi zostaną usunięte z App Store, a możliwość ich instalacji za pośrednictwem alternatywnego kanału dystrybucji zostanie zablokowana; może to też skutkować usunięciem Cię z programu Apple Developer Program.

5.6 Kodeks postępowania deweloperów ↪

Prosimy o traktowanie wszystkich z szacunkiem, zarówno w odpowiedziach na recenzje w App Store, prośby klientów o wsparcie, jak i podczas komunikacji z Apple, w tym w odpowiedziach w App Store Connect. Nie wolno angażować się w żadne formy nękania, praktyki dyskryminacyjne,

zastraszanie, prześladowanie ani zachęcać innych do angażowania się w którekolwiek z powyższych działań. Powtarzające się zachowania manipulacyjne, wprowadzające w błąd lub inne nieuczciwe działania będą skutkować usunięciem Cię z programu Apple Developer Program.

Zaufanie klientów jest fundamentem ekosystemu aplikacji. Aplikacje nigdy nie powinny żerować na użytkownikach ani próbować oszukiwać klientów, nakłaniać ich do niechcianych zakupów, zmuszać ich do udostępniania niepotrzebnych danych, podstępnie podnosić cen, pobierać opłat za funkcje lub treści, które nie są dostarczane, ani angażować się w jakiegokolwiek inne działania manipulacyjne w aplikacji lub poza nią.

Twoje konto w programie Developer Program zostanie zamknięte, jeśli podejmiesz aktywności lub działania niezgodne z kodeksem postępowania deweloperów. Aby przywrócić swoje konto, możesz złożyć pisemne oświadczenie opisujące ulepszenia, które zamierzasz wprowadzić. Jeśli plan zostanie zatwierdzony przez Apple, a my potwierdzimy wprowadzenie zmian, Twoje konto może zostać przywrócone.

5.6.1 Recenzje w App Store

Recenzje klientów App Store mogą być integralną częścią korzystania z aplikacji, dlatego należy traktować klientów z szacunkiem, odpowiadając na ich komentarze. Odpowiedzi powinny być ukierunkowane na komentarze użytkowników i nie powinny zawierać danych osobowych, spamu ani treści marketingowych.

Użyj dostarczonego interfejsu API, aby zachęcić użytkowników do wystawienia recenzji Twojej aplikacji. Ta funkcja pozwala klientom wystawiać oceny i recenzje w App Store bez niedogodności związanych z opuszczaniem aplikacji, a my nie będziemy zezwalać na niestandardowe zachęty do recenzowania.

5.6.2 Tożsamość dewelopera

Dostarczanie weryfikowalnych informacji Apple i klientom ma kluczowe znaczenie dla budowania zaufania klientów. Musisz dokładnie przedstawić siebie, swoją firmę i swoje oferty w App Store lub na alternatywnych platformach sprzedaży aplikacji. Informacje, które podajesz, muszą być prawdziwe, istotne i aktualne, aby Apple i klienci rozumieli, z kim mają do czynienia, i mogli się z Tobą skontaktować w razie jakichkolwiek problemów.

5.6.3 Wykrywanie oszustw

Uczestnictwo w App Store wymaga uczciwości i zaangażowania w budowanie oraz utrzymywanie zaufania klientów. Manipulowanie jakimkolwiek elementem doświadczenia klienta w App Store, takim jak listy przebojów, wyszukiwanie, recenzje lub odesłania do aplikacji, podważa zaufanie klientów i jest niedozwolone.

5.6.4 Jakość aplikacji

Klienci oczekują od App Store najwyższej jakości, a utrzymanie wysokiej jakości treści, usług i doświadczeń sprzyja ich zaufaniu. Sygnałami, że to oczekiwanie nie jest spełnione, są nadmierne zgłoszenia klientów dotyczące problemów z aplikacją, takie jak negatywne recenzje klientów oraz nadmierna liczba wniosków o zwrot pieniędzy. Niezdolność do utrzymania wysokiej jakości może być czynnikiem decydującym o tym, czy deweloper przestrzega Kodeksu Postępowania Dewelopera.

Po zgłoszeniu

Po zgłoszeniu aplikacji i metadanych w App Store Connect i rozpoczęciu procesu weryfikacji należy pamiętać o następujących kwestiach:

- **Czas:** Zespół App Review zweryfikuje Twoją aplikację tak szybko, jak to możliwe. Jeśli jednak Twoja aplikacja jest skomplikowana lub przedstawia nowe problemy, może wymagać dokładniejszej analizy i rozważenia. Pamiętaj też, że jeśli Twoja aplikacja jest wielokrotnie odrzucana z powodu tego samego naruszenia wytycznych lub próbujesz manipulować procesem weryfikacji, proces weryfikacji aplikacji potrwa dłużej. Dowiedz się więcej na temat [weryfikacji aplikacji](#).
- **Uaktualnienia statusu:** bieżący status Twojej aplikacji będzie odzwierciedlony w App Store Connect, więc możesz stamtąd obserwować sytuację.
- **Przyspieszone wnioski:** Jeśli masz krytyczny problem związany z czasem, możesz [poprosić o przyspieszoną weryfikację](#). Szanuj innych deweloperów i ubiegaj się o przyspieszoną weryfikację tylko wtedy, gdy naprawdę jej potrzebujesz. Jeśli stwierdzimy, że nadużywasz tego systemu, możemy odrzucać Twoje wnioski w przyszłości.
- **Data wydania:** Jeśli data wydania jest ustawiona na przyszłość, aplikacja nie pojawi się w App Store do tej daty, nawet jeśli zostanie zatwierdzona przez zespół App Review. Pamiętaj też, że może upłynąć do 24 godzin, zanim Twoja aplikacja pojawi się we wszystkich wybranych witrynach sklepowych.
- **Odrzucenia:** Naszym celem jest sprawiedliwe i konsekwentne stosowanie się do tych wytycznych, ale nikt nie jest doskonały. Jeśli Twoja aplikacja została odrzucona i masz pytania lub chcesz udzielić dodatkowych informacji, skorzystaj z usługi App Store Connect, aby skontaktować się bezpośrednio z zespołem App Review. Może to pomóc w udostępnieniu Twojej aplikacji w sklepie, a także w usprawnieniu procesu weryfikacji aplikacji lub zidentyfikowaniu potrzeby wyjaśnienia naszych zasad.
- **Odwołania:** Jeśli nie zgadzasz się z wynikiem weryfikacji, prosimy o [złożenie odwołania](#). Może to pomóc w umieszczeniu aplikacji w sklepie. Możesz również [zapropionować zmiany w samych wytycznych](#), aby pomóc nam usprawnić proces weryfikacji aplikacji lub dostrzec potrzebę doprecyzowania zasad.
- **Zgłaszanie poprawek:** W przypadku aplikacji, które już znajdują się w App Store lub na alternatywnych platformach sprzedaży aplikacji, poprawki błędów nie będą opóźniane z powodu naruszeń wytycznych, z wyjątkiem tych związanych z kwestiami prawnymi lub kwestiami bezpieczeństwa. Jeśli aplikacja została odrzucona i kwalifikuje się do tego procesu, skorzystaj z usługi App Store Connect, aby skontaktować się bezpośrednio z zespołem App Review, wskazując, że chcesz skorzystać z tego procesu i planujesz rozwiązać problem w kolejnym zgłoszeniu.

Z niecierpliwością czekamy na kolejne pomysły!

Ostatnia aktualizacja: [5 marca 2024 r.](#)