

Програмни правила за програмистите

(В сила от 5 март 2025 г., освен ако не е посочено друго)

Нека създадем най-надеждния източник за приложения и игри в света

Нововъведенията ви са в основата на общия ни успех, но с него идва и отговорността. Тези програмни правила за програмистите, наред със [Споразумението с програмистите относно разпространението](#), гарантират, че чрез Google Play заедно можем да продължим да предоставяме най-новаторските и надеждни приложения в света на над един милиард души. Приканваме ви да разгледате правилата ни по-долу.

Ограничено съдържание

Хора от цял свят ежедневно използват Google Play, за да осъществяват достъп до приложения и игри. Преди да изпратите дадено приложение, запитайте се дали е подходящо за услугата и дали спазва местните закони.

Застрашаване на деца

Приложения, които не забраняват на потребителите да създават, качват или разпространяват съдържание, което улеснява експлоатацията или насилието над деца, ще бъдат премахвани незабавно от Google Play. Това включва всички материали със сексуално насилие над деца. За да подадете сигнал за съдържание в продукт на Google, което може да експлоатира деца, кликнете върху [Подаване на сигнал за злоупотреба](#). Ако попаднете на такова съдържание другаде в интернет, моля, свържете се направо със [съответния орган в вашата страна](#).

Забраняваме използването на приложения за застрашаване на деца. Това включва, без изчерпването да е изчерпателно, използването на приложения за насърчаване на „хищническо“ поведение към деца, като например:

- неподходящо поведение, насочено към дете (например опипване или галене);
- подвеждане на деца с цел сексуална злоупотреба (например сприяеляване с дете онлайн с цел улесняване на сексуален контакт и/или обмен на сексуални изображения с него онлайн или офлайн);
- сексуализиране на непълнолетно лице (например изображения, които насърчават или популяризират сексуалното насилие над деца или изобразяването на деца по начин, който може да доведе до сексуална експлоатация на деца);
- сексуално изнудване (например заплахи или изнудване на дете чрез използване на реален или предполагаем достъп до интимни изображения на детето);
- трафик на деца (например рекламиране или установяване на контакт с дете с цел търговска сексуална експлоатация).

Ще предприемем подходящите действия, включително изпращане на сигнал до Националния център за изчезнали и експлоатирани деца, ако установим наличието на материали със сексуално насилие над деца. Ако смятате, че някое дете е в опасност или е било жертва на насилие, експлоатация или трафик на хора, се свържете с местните правоприлагащи органи и организация за защита на децата, посочена [тук](#).

Освен това не се допускат приложения, които са привлекателни за деца, но съдържат теми за пълнолетни, включително, но не само:

- приложения с твърде много насилие, кръв и жестокост;

- приложения, които изобразяват или насърчават вредни и опасни дейности.

Също така не допускаме приложения, които популяризират отрицателни изображения на физическия облик, включително такива, които с цел развлечение изобразяват пластични операции, отслабване и други козметични корекции на външния вид на даден човек.

Правила за стандартите за безопасност на децата

Google Play изисква социалните и приложенията за запознанства да спазват правилата ни за стандартите за безопасност на децата.

Тези приложения трябва да изпълняват следните изисквания:

- **Да имат публикувани стандарти:** Приложението ви трябва изрично да забранява сексуалното насилие над деца и сексуалната експлоатация на деца в публично достъпни стандарти, като например общите условия на приложението, правила на общността или друга публично достъпна документация за правилата за потребители.
- **Да предоставят механизъм за потребителски отзиви в приложението:** Трябва да сертифицирате самостоятелно, че предоставяте механизъм в рамките на приложението си, чрез който потребителите да изпращат отзиви, притеснения или сигнали.
- **Да вземат мерки срещу материалите със сексуално насилие над деца:** Трябва самостоятелно да сертифицирате, че приложението ви взема подходящите мерки, включително, без изброяването да е изчерпателно, премахване на материалите със сексуално насилие над деца, след като бъде получена действителна информация за такива материали, в съответствие с приложимото законодателство и публикуваните ви стандарти.
- **Да спазват законите за безопасност на децата:** Трябва самостоятелно да сертифицирате, че приложението ви спазва приложимите закони и разпоредби за безопасност на децата, включително, без изброяването да е изчерпателно, да разполагате с процедура за подаване на сигнали за потвърдени материали със сексуално насилие над деца до [Националния център за изчезнали и експлоатирани деца](#) или до [съответния ви регионален орган](#).
- **Да осигуряват лице за връзка относно безопасността на децата:** Приложението ви трябва да посочва конкретно лице за връзка, което да получава евентуалните известия от Google Play относно съдържание със сексуално насилие над деца и сексуална експлоатация на деца, открито в приложението или платформата ви. Това лице трябва да е в състояние при необходимост да прилага процедурите ви за преглед и налагане на мерки.

Научете повече за тези изисквания и как да ги спазвате в статията ни в [Помощния център](#).

Неподходящо съдържание

За да поддържа Google Play като безопасна и уважавана платформа, създадохме стандарти, дефиниращи и забраняващи съдържание, което е опасно или неуместно за потребителите ни.

Сексуално съдържание и непристоен език

Не допускаме приложения, които включват или популяризират сексуално съдържание или непристоен език, включително порнография, нито материали или услуги, предназначени да предизвикат сексуално удовлетворение. Не допускаме приложения или съдържание в тях, които изглежда, че популяризират или предлагат сексуален акт срещу възнаграждение. Не допускаме приложения, които включват или популяризират съдържание, свързано с „хищническо“ сексуално поведение, или разпространяват сексуално съдържание, споделено без съгласие. Може да допуснем съдържание с актови изображения, ако основната му цел е образователна, документална, научна или художествена и те не се използват безпричинно.

Приложенията за каталози – приложения, съдържащи списъци със заглавия на книги/ видеоклипове като част от по-широк каталог със съдържание – може да разпространяват книги (включително електронни и аудиокнизи) или видеоклипове със сексуално съдържание, при условие че са спазени следните изисквания:

- Книгите/видеоклиповете със сексуално съдържание представляват малка част от каталога на приложението.
- Приложението не популяризира активно книгите/видеоклиповете със сексуално съдържание. Съответните заглавия може да се показват в препоръките въз основа на историята на потребителя или при ценови промоции от общ характер.
- Приложението не разпространява книги/видеоклипове със съдържание, свързано със застрашаване на деца, порнография или друго сексуално съдържание, което е незаконно съгласно приложимото законодателство.
- Приложението предпазва непълнолетните лица, като ограничава достъпа до книгите/ видеоклиповете със сексуално съдържание.

Ако дадено приложение включва съдържание, което нарушава настоящите правила, но се смята за подходящо в конкретен регион, то може да бъде достъпно за потребителите там, но няма да е налице за потребителите в други региони.

Ето няколко примера за често срещани нарушения:

- Актове сексуални изображения или показване на пози, предизвикващи сексуални асоциации, в които обектът е гол, замъглен или с оскъдно облекло, което не би било приемливо в определен обществен контекст;
- Изображения, анимации или илюстрации на сексуални актове, пози, предизвикващи неприлични сексуални асоциации, или показване на части от тялото по сексуален начин;
- Материали, които изобразяват или представляват функционални сексуални помагала, сексуални ръководства, незаконни сексуални теми и фетиши;
- Съдържание, което е нецензурно или непристойно, включително, но не само, съдържание, което може да включва непристоен език, обиди, нецензурен текст или сексуални ключови думи или такива за пълнолетни в малката обява в магазина или в приложението;
- Съдържание, което изобразява, описва или насърчава към содомия;
- Приложения, популяризиращи развлечения, свързани със секс, компаньонски или други услуги, които могат да се тълкуват като предоставяне или предлагане на сексуални актове срещу възнаграждение, включително, но не само подаръци или заплащане срещу услуги на компаньонка или сексуални договорености, при които се подразбира или очаква единият участник да предостави пари, подаръци или финансова подкрепа на друг участник;
- Приложения, които унижават или обективират хората, като например такива, които заявяват, че събличат хора или че хората са с прозрачно облекло, дори ако са означени като приложения за развлечения или за шега;
- Съдържание или поведение, което се опитва да заплашва или експлоатира хората по сексуален начин, като например тайно направени снимки с интимен характер, скрита камера, сексуално съдържание без съгласието на участниците, създадено чрез дийпфейк или подобна технология, или съдържание с нападения.

Насаждане на омраза

Не допускаме приложения, които популяризират насилие или насаждат омраза спрямо човек или група от хора въз основа на тяхната раса, етнически произход, религия, увреждания, възраст, националност, военна служба, сексуална ориентация, пол, полова идентичност, каста, имиграционен статут или друга характеристика, свързана със системна дискриминация или маргинализиране.

Приложенията, които включват съдържание за нацизма с образователен, документален, научен или художествен характер, може да бъдат блокирани в определени държави съгласно

местни закони и разпоредби.

Ето няколко примера за често срещани нарушения:

- Съдържание или думи, които имат за цел да докажат, че защитена група хора са нисши, нечовеци или заслужаващи омраза;
- Приложения, които съдържат насаждащи омраза забележки, стереотипи или теории за защитена група с отрицателни характеристики (например злонамереност, корумпираност и др.) или изрично или косвено твърдят, че групата представлява заплаха;
- Съдържание или думи, които се опитват да насърчат групи хора да вярват, че определени лица трябва да бъдат мразени или дискриминирани, защото са членове на защитена група;
- Съдържание, което популяризира символи за насаждане на омраза, като например флагове, символи, емблеми, принадлежности или поведение, свързани с насаждащи омраза групи.

Насилие

Не допускаме приложения, които изобразяват или улесняват безпричинно насилие или други опасни дейности. Обикновено се допускат приложения, които изобразяват въображаемо насилие в контекста на игра, като например анимационни филми, лов или риболов.

Ето няколко примера за често срещани нарушения:

- Графично изобразяване или описание на реалистично насилие или на заплахи за насилие над хора или животни.
- Приложения, които популяризират самонараняване, самоубийство, разстройства на храненето, игри със задушаване или други действия, които може да доведат до сериозни наранявания или смърт.

Насилствен екстремизъм

Не разрешаваме на терористични организации или други опасни организации или движения, които са участвали в актове на насилие срещу граждани, подготвяли са такива или са поели отговорност за тях, да публикуват приложения в Google Play за каквито и да е цели, включително за набиране на членове.

Не допускаме приложения, чието съдържание е свързано с насилствен екстремизъм или с планиране, подготовка или възхвала на насилие срещу граждани, като например такова, което популяризира или възхвалява терористични нападения или подстрекава към насилие. Ако публикувате свързано с насилствен екстремизъм съдържание с образователна, документална, научна или художествена цел, не забравяйте да посочите съответен подходящ контекст.

Деликатни събития

Не допускаме приложения, в които се извлича изгода от или не се проявява деликатно отношение към деликатно събитие със значително социално, културно или политическо въздействие, като например опасности за населението, природни бедствия, извънредни ситуации, свързани с общественото здраве, конфликти, смъртни случаи или други трагични събития. Обикновено се допускат приложения, чието съдържание е свързано с деликатно събитие, ако съдържанието е с образователен, документален, научен или художествен характер или има за цел да предупреди потребителите за събитието или да повиши информираността им.

Ето няколко примера за често срещани нарушения:

- Липса на тактичност по отношение на смъртта на реален човек или група хора поради самоубийство, свръхдоза, естествени причини и др.
- Отричане на голямо трагично събитие, което е добре документирано.

- Евентуално облагодетелстване от деликатно събитие без видима полза за жертвите.

Малтретиране и тормоз

Не допускаме приложения, които улесняват заплахи, тормоз или малтретиране.

Ето няколко примера за често срещани нарушения:

- Малтретиране на жертвите на международни или религиозни конфликти;
- Съдържание, което има за цел да експлоатира други хора, включително изнудване, шантаж и др.;
- Публикуване на съдържание с цел публично унижаване на човек;
- Тормоз спрямо жертвите на трагично събитие или на техните приятели и семейства.

Опасни продукти

Не допускаме приложения, които улесняват продажбата на взривни вещества, огнестрелни оръжия, боеприпаси или определени оръжейни принадлежности.

- Ограничените принадлежности включват приспособления за импровизиране на автоматична стрелба или за преправяне на огнестрелно оръжие в автоматично (напр. устройства за ускоряване на стрелбата, спусъци и приставки за автоматична стрелба, комплекти за преправяне), както и пълнители или ленти с над 30 патрона.

Не допускаме приложения, които дават указания за производството на взривни вещества, огнестрелни оръжия, боеприпаси, ограничени оръжейни принадлежности или други оръжия. Това включва инструкции за преправяне на огнестрелно оръжие в автоматично или за импровизиране на автоматична стрелба.

Марихуана

Не допускаме приложения, които улесняват продажбата на марихуана или продукти от марихуана независимо от тяхната законност.

Ето няколко примера за често срещани нарушения:

- Даване на възможност на потребителите да поръчват марихуана чрез функцията за пазарска кошница в приложението.
- Подпомагане на потребителите при организирането на доставка или получаване на марихуана.
- Улесняване на продажбата на продукти, които съдържат тетрахидроканабиол (THC), включително продукти като конопено масло (канабидиол) със съдържание на THC.

Тютюневи изделия и алкохол

Не допускаме приложения, които улесняват продажбата на тютюневи изделия или продукти, съдържащи никотин (като например електронни цигари, вейп устройства и никотинови паучове), или насърчават незаконната или неуместната употреба на алкохол, тютюневи изделия или никотин.

Допълнителна информация

- Не се допуска изобразяването или насърчаването на употребата или продажбата на алкохол или тютюн на непълнолетни лица.
- Не се допуска внушаването, че употребата на тютюневи изделия може да подобри представянето в социално, сексуално, професионално, интелектуално или спортно отношение.

- Не се допуска представянето на прекомерната употреба на алкохол в благоприятна светлина, включително изобразяването, насърчаващо прекомерно и прекалено пиене или надпиване.
 - Не се допуска рекламирането, популяризирането или представянето на видно място на тютюневи изделия (това включва реклами, банери, категории и връзки към сайтове за продажба на тютюн).
 - В определени региони може да разрешим ограничената продажба на тютюневи изделия в приложенията за доставка на храна и хранителни стоки, при условие че имат предпазни мерки за контрол на възрастта (като например проверка на самоличността при доставка).
 - Може да разрешим продажбата на продукти, популяризирани като помощ за спиране на никотина, при условие че имат предпазни мерки за контрол на възрастта.
-

Финансови услуги

Не допускаме приложения, които излагат потребителите на измамни или опасни финансови продукти и услуги.

За целите на настоящите правила за финансови продукти и услуги смятаме онези, свързани с управлението или инвестирането на пари и криптовалути, включително персонализираните съвети.

Ако приложението ви съдържа или популяризира финансови продукти и услуги, трябва да спазвате държавните и местните разпоредби във всеки регион или държава, към които е насочено, например да разкриете конкретна информация според изискванията на местното законодателство.

За приложенията, които съдържат финансови функции, трябва да се попълни формулярът за декларирането им в [Play Console](#).

Бинарни опции

Не допускаме приложения, които дават на потребителите възможност да търгуват с бинарни опции.

Потребителски заеми

За потребителски заем следва да се приема еднократното предоставяне на пари назаем от физическо лице, организация или юридическо лице на физическо лице, но не с цел да се финансира обучение в учебно заведение или закупуването на дълготраен актив. На потребителите на лични заеми е необходима информация за качеството, характеристиките, таксите, графика за погасяване, рисковете и предимствата на заемните продукти, за да вземат информирани решения за това, дали да вземат заема.

- Примери: потребителски заеми, заеми до заплата, заеми без посредник, заеми срещу право на собственост.
- Не са включени: ипотечи, заеми за покупка на автомобил, револвиращи кредитни линии (като например кредитни карти, лични кредитни линии).

Приложенията, които предоставят потребителски заеми, включително, но не само, такива, които предлагат заеми директно, тези за генериране на възможни клиенти, както и тези, които свързват потребителите със заемодатели трети страни, трябва да бъдат в категория „Финанси“ в Play Console и да разкриват следната информация в метаданните си:

- минимален и максимален срок за погасяване на заема;
- максимален годишен процент на разходите (ГПР), който обикновено включва лихвения процент плюс такси и други разходи за година, или друг подобен процент, който се

изчислява в съответствие с местното законодателство;

- представителен пример за общата стойност на заема с включена главница и всички приложими такси;
- декларация за поверителност, която изчерпателно описва достъпа, събирането, използването и споделянето на лични и поверителни потребителски данни, като тези действия са в рамките на ограниченията на настоящите правила.

Не допускаме приложения, популяризиращи потребителски заеми, които трябва да бъдат изплатени напълно в рамките на 60 дни или по-малко от датата на отпускане на заема (наричаме ги „краткосрочни потребителски заеми“).

Изключения от това правило се допускат за приложения за потребителски заеми, насочени към държави, в които отдаването на подобни краткосрочни заеми е изрично разрешено чрез конкретни разпоредби и съгласно установени правни рамки. В тези редки случаи възможността за изключение ще бъде разгледана в съответствие с приложимите местни закони и разпоредби на съответната държава.

Трябва да сме в състояние да установим връзка между профила ви на програмист и предоставените лицензи или документи, доказващи, че имате право да предоставяте потребителски заеми. Може да поискаме допълнителна информация или документи за потвърждение, че профилът ви спазва всички местни закони и разпоредби.

Приложенията за потребителски заеми, тези, чиято основна цел е улесняване на достъпа до такива заеми (например посредници или генератори на възможни клиенти), аксесоарните приложения за заеми (калкулатори за заеми, ръководства за заеми и др.) и приложенията за авансови трудови възнаграждения (EWA) нямат право да осъществяват достъп до чувствителни данни, като например снимки и контакти. Следните разрешения са забранени:

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

Приложенията, които използват поверителна информация или API, са предмет на допълнителни ограничения и изисквания. За допълнителна информация разгледайте [правилата относно разрешенията](#).

Потребителски заеми с висок ГПР

В САЩ не допускаме приложения, които предлагат потребителски заеми с годишен процент на разходите (ГПР) от 36% или по-висок. Приложенията за потребителски заеми в САЩ трябва да показват максималния ГПР, изчислен в съответствие със [Закона за честно кредитиране \(TILA\)](#) .

Това правило се отнася за приложенията, които предлагат заеми директно, приложенията за генериране на възможни клиенти, както и тези, които свързват потребителите със заемодатели трети страни.

Изисквания за конкретни държави

Приложения за потребителски заеми, които са насочени към изброените държави, трябва да изпълняват допълнителни изисквания и да предоставят още документация като част от декларацията за финансови функции в [Play Console](#). При поискване от Google Play трябва да

предоставите допълнителна информация или документи, които подкрепят това, че спазвате приложимите регулаторни изисквания и тези за лицензиране.

1. Индия

- Ако имате лиценз от Reserve Bank of India (RBI) за предоставяне на потребителски заеми, трябва да изпратите негово копие за проверка.
- Ако не давате заеми директно, а само осигурявате платформа за улесняване на предоставянето им на потребителите от регистрирани небанкови финансови компании или банки, трябва да посочите това в декларацията.
- Освен това имената на всички регистрирани небанкови финансови компании и банки трябва да бъдат разкрити по ясен начин в описанието на приложението ви.

2. Индонезия

- Ако приложението ви предлага услуги за даване на заеми въз основа на информационни технологии съгласно разпоредба № 77/ПОЖК.01/2016 на ОЖК (която може да бъде периодично променяна), трябва да ни изпратите за проверка копие на валидния си лиценз.

3. Филипини

- Всички финансови и кредитни компании, които предлагат заеми чрез онлайн платформи за заем (OLP), трябва да получат регистрационен номер от SEC и номер на сертифициращ орган от Комисията по ценните книжа и борсите на Филипините (PSEC).
- Освен това, за да действате като финансова/кредитна компания, в описанието на приложението си трябва да разкриете своето корпоративно име, име на бизнеса, регистрационен номер от PSEC и сертифициращ орган.
- Приложенията, които предлагат групово финансиране под формата на заеми, като например заеми чрез P2P платформи, или съгласно дефиницията в Правилата и разпоредбите за групово финансиране, трябва да обработват транзакциите чрез регистрирани в PSEC посредници за групово финансиране.

4. Нигерия

- Дигиталните заемодатели трябва да спазват ОГРАНИЧЕНАТА ВРЕМЕННА РЕГУЛАТОРНА/РЕГИСТРАЦИОННА РАМКА И УКАЗАНИЯТА ЗА ДИГИТАЛНО КРЕДИТИРАНЕ, 2022 г. (може периодично да бъдат променяни) и да попълнят съответния формуляр на Федералната комисия на Нигерия по защита на конкуренцията и потребителите (FCCPC), както и да получат писмо от FCCPC за одобрение, което може да бъде проверено.
- Агрегаторите на заеми трябва да предоставят документация и/или сертификат за услуги за дигитално кредитиране и контакти за връзка за всеки DML, с който си партнират.

5. Кения

- Дигиталните кредитори трябва да завършат съответния регистрационен процес и да получат лиценз от Централната банка на Кения (CBK). Като част от декларацията трябва да предоставите копие на лиценза си от CBK.
- Ако не давате заеми директно, а само осигурявате платформа за улесняване на предоставянето им на потребителите от регистрирани дигитални кредитори, трябва да посочите това в декларацията и да предоставите копия на притежаваните от партньорите лицензи за дигитални кредитори.
- Понастоящем приемаме декларации и лицензи само от юридически лица в регистъра за дигитални кредитори в официалния уебсайт на CBK.

6. Пакистан

- Заемодател, който е небанкова финансова компания (NBFC), може да публикува само едно приложение за дигитално кредитиране (DLA). Програмистите, които опитат да

публикуват повече от едно DLA за една NBFC, рискуват профилът им на програмист и всички други свързани профили да бъдат прекратени.

- За да предлагате или посредничите за услуги за дигитално кредитиране в Пакистан, трябва да изпратите доказателство за одобрение от SECP.

7. Тайланд

- Приложенията за потребителски заеми, насочени към Тайланд, с лихва от 15% или повече, трябва да имат валиден лиценз от Тайландската банка (BoT) или Министерството на финансите (MoF). Програмистите трябва да предоставят документи, доказващи, че имат право да предоставят потребителски заеми в Тайланд или да посредничат за това. Тези документи включват:
 - копие на лиценза им от Тайландската банка, разрешаващ да извършват дейност като кредитор на потребителски заеми или нанофинансова организация;
 - копие на бизнес лиценза им, издаден от Министерството на финансите, разрешаващ да извършват дейност като заемодатели на малки заеми тип Pico или Pico-plus.

Ето пример за често срещано нарушение:

< Back

Easy Loans
offers in app purchases

★★★★★ 1255

Install

Are you looking for a speedy loan?

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

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

Violations

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

Хазарт, игри и състезания с истински пари

Разрешаваме приложения за хазарт с истински пари, реклами, свързани с хазарт с истински пари, програми за лоялност с елементи на игра и приложения за дневен фентъзи спорт, които отговарят на определени изисквания.

Приложения за хазарт

В съответствие с ограниченията и при условие че са спазени всички правила на Google Play, допускаме в определени държави приложения, които улесняват или са предназначени за онлайн хазарт, стига програмистът [да завърши процеса на кандидатстване](#) за разпространение на съответното приложение в Google Play, да е одобрен правителствен оператор и/или да е регистриран като лицензиран оператор при съответния

правителствен орган по хазарта в посочената държава, и да предостави валиден лиценз за дейност в посочената държава за типа продукт за онлайн хазарт, който иска да предлага.

Допускаме само валидни лицензирани или упълномощени приложения за хазарт, които предлагат следните типове продукти за онлайн хазарт:

- Онлайн казино игри
- Спортни залагания
- Конни надбягвания (където са регламентирани и лицензирани отделно от спортните залагания)
- Лотарии
- Дневни фентъзи спортове.

Отговарящите на условията приложения трябва да изпълнят следните изисквания:

- Програмистът трябва успешно [да завърши процеса на кандигатстване](#), за да разпространява приложението в Google Play.
- Приложението трябва да спазва всички приложими закони и отраслови стандарти за всяка държава, където се разпространява.
- Програмистът трябва да има валиден лиценз за хазарт за всяка държава или щат/територия, в които се разпространява приложението.
- Програмистът не трябва да предлага хазартен продукт от тип, който не е в обхвата на съответния лиценз за хазарт.
- Приложението не бива да позволява на непълнолетни потребители да го използват.
- Приложението не трябва да позволява достъп и използване от държави, щати/територии или географски райони, необхванати от лиценза за хазарт, предоставен от програмиста.
- Приложението НЕ бива да може да се купи като платено приложение в Google Play, нито да използва въграденото таксуване чрез Google Play.
- Приложението трябва да се изтегля и инсталира от Google Play Магазин без парично заплащане.
- Приложението трябва да е с класификация АО („Само за пълнолетни“) или [еквивалентна от IARC](#).
- Приложението и малката му обява трябва ясно да показват информация за отговорно отношение към хазарта.

Други приложения за игри, състезания и турнири с истински пари

За всички други приложения, които не отговарят на описаните по-горе условия за приложенията за хазарт и не са включени в „Пилотни програми за други игри с истински пари“ по-долу, не допускаме съдържание или услуги, които дават възможност на потребителите или ги улесняват да правят облози, да залагат или да участват с истински пари (включително купени с пари елементи в приложения), за да получат реални парични награди. Това включва, без изброяването да е изчерпателно, онлайн казина, спортни залагания, лотарии и игри, които приемат пари и предлагат парични или други материални награди (освен програмите, разрешени съгласно описаните по-долу изисквания за програми за лоялност с елементи на игра).

Примери за нарушения

- Игри, които приемат пари в замяна на възможността за спечелване на физическа или парична награда.
- Приложения, които имат елементи или функции за навигация (напр. елементи от меню, раздели, бутони, [елементи WebView](#) и др.), които предоставят „подканваща фраза“ за правене на облози, залагане или участие в игри, състезания или турнири с истински пари, като например приложения, които подканват потребителите да залагат, да се регистрират или състезават в турнир за шанса да спечелят парична награда.

- Приложения, които приемат или управляват залагания, валути в приложението, печалби или депозити в замяна на физическа или парична награда или на възможността за получаване на такава.

Пилотни програми за други игри с истински пари

Понякога в избрани региони може да провеждаме пилотни програми за ограничен период от време за определени типове игри с истински пари. За подробности разгледайте тази страница в [Помощния център](#). Пилотната програма в Япония за онлайн игри за хващане на награди завърши на 11 юли 2023 г. От 12 юли 2023 г. в Google Play може да има малки обяви за приложенията за онлайн машини за хващане на награди, които да се виждат в цял свят, при условие че са спазени приложимите закони и определени [изисквания](#).

Програми за лоялност с елементи на игра

Където това е разрешено от закона и не е предмет на допълнителни изисквания за лицензиране на хазарт или игри, разрешаваме програми за лоялност, които поощряват потребителите с истински награди или парични еквиваленти, ако отговарят на следните условия за Google Play Магазин:

За всички приложения (игри и др.):

- Трябва да бъде ясно, че предимствата, поощренията или наградите в програмата за лоялност се предоставят допълнително и след извършване на отговаряща на условията парична транзакция в приложението (която трябва да бъде действителна отделна транзакция за предоставяне на стоки или услуги извън програмата за лоялност). Също така те не трябва да се предлагат за покупка, нито да се търгуват по друг начин, тъй като това би било нарушение на ограниченията в правилата за хазарт, игри и състезания с истински пари.
- Например никоя част от отговарящата на условията парична транзакция не може да представлява такса или залог за участие в програмата за лоялност, а самата транзакция не трябва да води до покупка на стоки или услуги на по-висока от обичайната цена.

За приложения, които са игри :

- Точките или наградите за лоялност с предимства, поощрения или награди, свързани с отговаряща на условията парична транзакция, може да се предоставят и осребряват само въз основа на фиксиран брой взаимодействия, който трябва да бъде ясно документиран в приложението и в общодостъпните официални правила за програмата. Освен това получаването на предимствата или съответната стойност **не трябва** да е свързано със залагане, нито да се определя от представянето в играта или въз основа на резултати, получавани на случаен принцип.

За приложения, които не са игри:

- Точките или наградите за лоялност може да са обвързани със състезание или резултати, получавани на случаен принцип, ако са изпълнени долупосочените изисквания. Програмите за лоялност с предимства, поощрения или награди, свързани с отговаряща на условията парична транзакция, трябва да изпълняват следните изисквания:
 - Да имат публикувани официални правила в приложението.
 - За програмите с променливи, основаващи се на шанс или рандомизирани системи за поощрения: в официалните условия на програмата трябва да бъдат разкрити 1) вероятностите за поощрителните програми, в които за определяне на поощренията се ползват фиксирани вероятности, и 2) начинът на избор (напр. променливите, служещи за определяне на поощрението) за другите такива програми.
 - В официалните условия на програмите, които предлагат промоции на лотариен или друг подобен принцип, трябва да са посочени фиксиран брой победители, определен краен

срок за участие и дата на връчване на наградата за всяка промоция.

- В приложението и в официалните условия на програмата трябва ясно да е документирано фиксирано съотношение за получаване и осребряване на точки или награди за лоялност.

Тип приложение с програма за лоялност	Елементи на игра в програмата за лоялност и различни награди	Награди за лоялност въз основа на фиксиран брой взаимодействия/ график	Общи условия на програмата за лоялност	Общите условия трябва да разкриват начина на избор или вероятността за спечелване на награди, ако те се предоставят на случаен принцип
Игра	Не са разрешени	Разрешени	Задължителни	Неприложимо (програмите за лоялност на приложения, които са игри, не може да работят на случаен принцип)
Друго	Разрешени	Разрешени	Задължителни	Задължително

Реклами за хазарт или игри, състезания и турнири с истински пари в приложения, разпространявани през Google Play

Допускаме приложения, които съдържат реклами, популяризиращи хазарт, или игри, състезания и турнири с истински пари, ако отговарят на следните изисквания:

- Приложението и рекламата (включително съответните рекламодатели) трябва да спазват всички приложими закони и отраслови стандарти за всяко местоположение, в което се показва рекламата.
- Рекламата трябва да спазва приложимите местни изисквания за лицензиране за всички свързани с хазарт продукти и услуги, които се популяризират.
- В приложението не бива да се показва реклама за хазарт на лица, за които е известно, че са под 18-годишна възраст.
- Приложението не трябва да е част от програмата „Приложения за семейството“.
- Приложението не бива да е насочено към лица под 18-годишна възраст.
- Ако се рекламира приложение за хазарт (според определението по-горе), рекламата трябва ясно да показва информация за отговорно отношение към хазарта на целевата страница, в приложението или в самата малка обява за рекламираното приложение.
- Приложението не трябва да предоставя съдържание, което наподобява хазартни игри (напр. социални казино приложения, приложения с виртуални ротативки).
- Приложението не трябва да осигурява поддръжка или придружаваща функционалност за хазарт или игри, лотарии или турнири с истински пари (напр. функция, която подпомага залаганията, изплащанията, проследяването на спортни резултати/коэффициенти/представяния или управлението на средствата за участие).
- Съдържанието на приложението не трябва да популяризира хазартни услуги или игри, лотарии или турнири с истински пари, нито да насочва потребителите към такива.

Само приложения, които отговарят на всички изисквания в съответната секция по-горе, може да включват реклами за хазарт или игри, лотарии или турнири с истински пари. Приеманите приложения за хазарт (според определението по-горе) или за дневен фентъзи спорт (според определението по-долу), които отговарят на изисквания от 1 до 6 по-горе, може да включват реклами за хазарт или игри, лотарии или турнири с истински пари.

Примери за нарушения

- Приложение, предназначено за непълнолетни потребители, в което се показва реклама, популяризираща хазартни услуги.
- Казино симулатор, който популяризира казина с истински пари или насочва потребителите към такива.
- Специално приложение за проследяване на спортни коефициенти, което съдържа интегрирани реклами за хазарт, водещи към сайт за спортни залагания.
- Приложения с реклами за хазарт, които нарушават правилата ни за [погвеждащите реклами](#), като например реклами, които се показват на потребителите като бутони, икони или други интерактивни елементи в приложението.

Приложения за дневен фентъзи спорт

Разрешаваме само определените от приложимото местно законодателство приложения за дневен фентъзи спорт, ако отговарят на следните изисквания:

- Приложението 1) се разпространява само в САЩ или 2) отговаря на условията съгласно горепосочените изисквания за приложенията за хазарт и процеса на кандидатстване за държави, различни от САЩ;
- Програмистът трябва успешно да завърши процеса на [кандидатстване за дневен фентъзи спорт](#) и приложението да бъде прието, за да се разпространява в Google Play;
- Приложението трябва да спазва всички приложими закони и отраслови стандарти за държавите, в които се разпространява;
- Приложението не бива да позволява на непълнолетни потребители да залагат или да извършват парични транзакции с него;
- Приложението НЕ бива да може да се купи като платено приложение в Google Play, нито да използва вграденото таксуване чрез Google Play;
- Приложението трябва безплатно да се изтегля и инсталира от Google Play Магазин;
- Приложението трябва да е с класификация АО („Само за пълнолетни“) или [еквивалентна от IARC](#);
- Приложението и малката му обява трябва ясно да показват информация за отговорно отношение към хазарта;
- Приложението трябва да спазва всички приложими закони и отраслови стандарти за всеки щат или територия на САЩ, където се разпространява;
- Програмистът трябва да има валиден лиценз за всеки щат или територия на САЩ, където се изисква такъв за приложения за дневен фентъзи спорт;
- Приложението не бива да позволява използване от щати или територии на САЩ, за които програмистът няма необходимия лиценз за приложения за дневен фентъзи спорт;
- Приложението не бива да позволява използване от щати или територии на САЩ, където приложенията за дневен фентъзи спорт са незаконни.

Незаконни дейности

Не допускаме приложения, които улесняват или популяризират незаконни дейности.

Ето няколко примера за често срещани нарушения:

- Улесняване на продажбата или покупката на незаконни наркотици.
 - Изобразяване или насърчаване на употребата или продажбата на наркотични вещества, алкохол или тютюн от непълнолетни лица.
 - Инструкции за отглеждането или производството на незаконни наркотици.
-

Съдържание, генерирано от потребителите

Съдържанието, генерирано от потребителите, е такова, което потребителите предоставят на приложението, като то се вижда или до него имат достъп поне някаква част от потребителите на приложението.

Приложенията, които съдържат или представят генерирано от потребителите съдържание, включително такива, които са специализирани браузъри или клиентски програми за насочване на потребителите към платформи за генерирано от потребителите съдържание, трябва да реализират ефективно, надеждно и постоянно модериране на това съдържание, което:

- изисква потребителите да приемат общите условия и/или правилата за потребителите на приложението, преди да могат да създават или да качват генерирано от тях съдържание.
- дефинира непристойното съдържание и поведение (по начин, който спазва програмните правила за програмистите в Google Play) и ги забранява в общите условия на приложението или в правилата за потребителите.
- извършва модериране на генерираното от потребителите съдържание в рамките на разумното и в съответствие с типа такова съдържание в приложението. Това включва осигуряване на система в приложението, служеща за подаване на сигнали и блокиране на потребители и на непристойно съдържание, генерирано от потребителите, както и вземане на мерки срещу потребителите или въпросното съдържание, когато това е уместно. Различните начини на работа с генерирано от потребителите съдържание може да изискват различни типове модериране. Например:
 - Приложенията с генерирано от потребителите съдържание, които идентифицират определен набор от потребители чрез средства като потвърждаване на потребителите или онлайн регистрация (например приложения, използвани изключително в рамките на определено учебно заведение или компания и т.н.), трябва да предоставят в себе си функционалност за подаване на сигнали за съдържанието и потребителите.
 - Функциите за генерирано от потребителите съдържание, които позволяват индивидуално взаимодействие между конкретни потребители (например директни съобщения, споменавания, маркиране), трябва да се предоставят заедно с функционалност в приложението, служеща за блокиране на потребители.
 - Приложенията, които осигуряват достъп до публично достъпно генерирано от потребителите съдържание, като например приложения за блогъри и за социални мрежи, трябва да реализират в себе си функционалност за подаване на сигнали за съдържание и за потребители и за блокиране на потребители.
 - В случаите на приложения с обогатена реалност (AR) модерирането на генерираното от потребителите съдържание (включително системата за сигнали в приложението) трябва да обхваща както непристойното съдържание с AR, генерирано от потребителите (напр. сексуално ориентирано нецензурно изображение с AR), така и деликатните местоположения за фиксиране на AR (напр. съдържанието с AR е фиксирано в ограничен район, като например военна база, или в частна собственост, където фиксирането на AR може да доведе до проблеми за собственика на имота).
- Нужно е предоставянето на предпазни мерки, чрез които да се предотврати насърчаването на нежелано поведение на потребителите от функцията за осигуряване на приходи в приложението.

Инцидентно сексуално съдържание

Сексуалното съдържание се счита за „инцидентно“, ако се показва в приложение с генерирано от потребителите съдържание, което (1) предоставя достъп основно до несексуално съдържание и (2) не популяризира активно, нито препоръчва сексуално съдържание. Сексуалното съдържание, което е дефинирано като незаконно от приложимото

законодателство, и съдържанието, описано на страницата [Застрашаване на деца](#), не се смята за „инцидентно“ и не се допуска.

Приложенията с генерирано от потребителите съдържание може да включват инцидентно сексуално съдържание, ако са изпълнени всички от следните изисквания:

- Съответното съдържание е скрито по подразбиране чрез филтри, за чието пълно деактивиране се изискват поне две потребителски действия (например чрез маскираща заставка или скрито по подразбиране, освен ако функцията Безопасно търсене не е деактивирана).
- Достъпът на деца (съгласно дефиницията в [правилата за семейства](#)) до приложението ви е изрично забранен чрез системи за отсяване по възраст, като например [неутрално отсяване по възраст](#) или подходяща система според приложимото законодателство.
- Приложението ви дава точни отговори във въпросника за класификация на генерираното от потребителите съдържание, както се изисква от [съответните правила](#).

Приложенията, чиято основна цел е да представят непристойно съдържание, генерирано от потребителите, ще бъдат премахвани от Google Play. Аналогично, приложенията, които в крайна сметка се използват основно за хостване на непристойно съдържание, генерирано от потребителите, или които си спечелят репутация сред потребителите на места, където е разпространено такова съдържание, също ще бъдат премахвани от Google Play.

Ето няколко примера за често срещани нарушения:

- Популяризиране на нецензурно сексуално ориентирано съдържание, генерирано от потребителите, включително внедряване или позволяване на платени функции, които предимно насърчават споделянето на непристойно съдържание;
- Приложения с генерирано от потребителите съдържание, които не разполагат с достатъчни предпазни мерки срещу заплахи, тормоз или малтретиране, особено към непълнолетни лица;
- Публикации, коментари или снимки в рамките на дадено приложение, чиято основна цел е тормоз над друго лице или набелязването му за злоупотреба, злонамерена атака или подигравка;
- Приложенията, които постоянно не реагират на жалбите на потребителите относно непристойно съдържание.

Здравно съдържание и услуги

Не допускаме приложения, които излагат потребителите на опасно здравно съдържание и услуги.

Ако приложението ви включва или популяризира здравно съдържание и услуги, то трябва да спазва приложимите закони и разпоредби.

Приложения за здраве

Ако приложението ви осъществява достъп до данни за здравословното състояние и е [здравно приложение](#) или предлага функции, свързани със здравето, то трябва да спазва съществуващите правила за програмисти в Google Play, включително правилата относно [поверителността, измамите и злоупотребите](#) и тези относно деликатните събития, в допълнение към изискванията по-долу:

• Декларация в Play Console:

- Отворете страницата „Съдържание на приложението“ („Правила > Съдържание на приложението“) в Play Console и изберете категорията или категориите, към които спада приложението ви.

- **Декларация за поверителност и изисквания за разкриване на информация по ясен начин:**

- Трябва да публикувате връзка към декларация за поверителност за приложението си в предназначенията за целта поле в Play Console, а в самото приложение – текста на декларацията или връзка към нея. Тя трябва да е публикувана на активен и достъпен за всички URL адрес без геозониране (не във формат PDF) и да е без възможност за редактиране (съгласно [секцията за безопасност на данните](#)).
- Декларацията за поверителност трябва, заедно с разкриванията на информация в приложението, изчерпателно да описва достъпа до [лични или поверителни потребителски данни](#), тяхното събиране, използване и споделяне. Това не се отнася само за данните, описани в секцията за безопасност на данните. За всички функционалности или данни, регулирани чрез [опасни разрешения или такива по време на изпълнение](#), приложението трябва да изпълнява всички приложими [изисквания за разкриване на информация по ясен начин и получаване на съгласие](#).
- Не трябва да се искат разрешения, които не са необходими за основната функционалност на здравното приложение, а неизползваните разрешения трябва да бъдат премахнати. За да видите списък с разрешенията, които попадат в обхвата за чувствителни данни, разгледайте [Категории приложения за здравето и допълнителна информация](#).
- Ако основната цел на приложението ви не е свързана със здравето, но то притежава съответните функции и осъществява достъп до данни за здравословното състояние, то пак попада в обхвата на правилата за здравните приложения. Връзката между основната функционалност на приложението и събирането на свързани със здравословното състояние данни (например застрахователи, приложения за игри, които събират данни за активността на потребителя, така че той да напредва в играта, и др.) трябва да е ясна за потребителя. Декларацията за поверителност на приложението трябва да отразява тези ограничени начини на ползване.

- **Допълнителни изисквания:**

Ако здравното ви приложение отговаря на някое от определенията по-долу, трябва да бъдат спазени съответните изисквания в допълнение към избирането на подходящата категория в Play Console:

- **Свързани с правителството здравни приложения:** Ако имате разрешение от правителството или призната здравна организация да разработвате и разпространявате приложение в партньорство с тях, трябва да изпратите доказателство, че отговаряте на условията, чрез [формуляра за предварително известие](#).
- **Приложения за здравословното състояние/проследяване на контактите:** Ако приложението ви служи за проследяване на контактите и/или установяване на здравословното състояние, изберете категорията за превенция на заболявания и обществено здравеопазване в Play Console и предоставете необходимата информация чрез формуляра за предварително известие по-горе.
- **Приложения за проучвания с хора:** Приложенията за провеждане на свързани със здравето проучвания с хора трябва да спазват всички правила и регламенти, включително, без изброяването да е изчерпателно, получаване на информирано съгласие от участниците или от родител или настойник, ако се касае за непълнолетно лице. Приложенията за свързани със здравето проучвания трябва да получат одобрение и от Бюро за проверка на институции (IRB) и/или еквивалентна независима комисия по етика, ако не са освободени от това по друг начин. Доказателство за такова одобрение трябва да бъде предоставено при поискване.
- **Приложения, изпълняващи ролята на медицинско устройство (SaMD):** Приложенията, които се смятат за медицински устройства (SaMD), трябва да получат удостоверяващо писмо или друг документ за одобрение, предоставен от регулаторен или друг орган, отговорен за управлението на здравното приложение и спазването на изискванията от

негова страна. При поискване трябва да бъде предоставено доказателство за наличието на съответното удостоверение или одобрение.

Данни от Health Connect

Данните, достъпни чрез разрешенията за Health Connect, се смятат за лични и поверителни потребителски данни, които са предмет на правилата относно [потребителските данни](#) и на [допълнителни изисквания](#).

Лекарства, изискващи лекарско предписание

Не допускаме приложения, които улесняват продажбата или покупката на лекарства, изискващи лекарско предписание, без представяне на рецепта.

Неодобри вещества

В Google Play не се допускат приложения, в които се популяризират или продават неодобри вещества, независимо от претенциите за законност.

Ето няколко примера за често срещани нарушения:

- Всички продукти в този неизчерпателен списък на [забранени фармацевтични продукти и хранителни добавки](#);
- продукти, съдържащи ефедра;
- продукти, съдържащи човешки хорионичен гонадотропин (hCG) във връзка със загуба/поддържане на теглото или когато се популяризират заедно с анаболни стероиди;
- билкови и хранителни добавки с активни фармацевтични или опасни съставки;
- фалшиви или заблуждаващи твърдения за ползност за здравето, включително такива, в които се загатва, че даден продукт е не по-малко ефективен от лекарствени средства, отпускани с рецепта, или контролирани вещества;
- продукти, които не са одобрени от правителствени органи и чийто маркетинг загатва, че са безопасни или ефективни при профилактиката, излекуването или лечението на дадена болест или неразположение;
- продукти, които са били предмет на правителствено или регулаторно действие или предупреждение;
- продукти с имена, които приличат на и може да бъдат сбъркани с тези на неодобри фармацевтични продукти, хранителни добавки или контролирани вещества.

За допълнителна информация относно неодобренията или заблуждаващи фармацевтични продукти и хранителни добавки, които наблюдаваме, моля, посетете www.legitscript.com.

Дезинформация във връзка със здравето

Не допускаме приложения, съдържащи подвеждащи твърдения за здравето, които противоречат на утвърдени медицински становища или могат да навредят на потребителите.

Ето няколко примера за често срещани нарушения:

- Подвеждащи твърдения относно ваксини – например че ваксините могат да променят ДНК.
- Защищаване на опасни и недоказани лечения.
- Защищаване на други опасни практики, свързани със здравето, като например репаративна терапия.

Медицински функционалности

Не разрешаваме приложения с медицински или свързани със здравето функции, които са подвеждащи или потенциално опасни. Не допускаме например приложения, които твърдят, че предлагат оксиметрия единствено въз основа на приложението. Приложенията оксиметри трябва да се поддържат от външен хардуер, носими аксесоари или специални сензори на смартфона, създадени да поддържат тази функционалност. Също така в метаданните на тези поддържани приложения трябва да има отказ от отговорност, в който се посочва, че не са предназначени за медицинска употреба, а само за осведомяване за общото физическо благосъстояние, и не представляват медицинско оборудване, а също така трябва да се разкрива по ясен начин моделът на съвместим хардуер/устройство.

Плащания – Клинични услуги

За транзакциите, включващи регулирани клинични услуги, не трябва да се използва системата на Google Play за таксуване. За повече информация разгледайте [Запознаване с правилата на Google Play за плащанията](#).

Базирано на блокчейн съдържание

Тъй като блокчейн технологията продължава да се развива бързо, се стремим да предоставяме максимално удобна за програмистите платформа, където да внедряват иновации и да създават по-добра и всеобхватна практическа работа за потребителите.

За целите на настоящите правила смятаме, че базираното на блокчейн съдържание представлява заместени с означение дигитални активи, защитени в блокчейн. Ако в приложението ви има такова съдържание, трябва да спазвате тези изисквания.

Борси за криптовалUTI и софтуерни портфейли

Купуването, съхраняването и обменът на криптовалута трябва да се извършват чрез сертифицирани услуги в регулирани юрисдикции.

Също така трябва да спазвате приложимите разпоредби във всеки регион или държава, към които е насочено приложението ви, и да не го публикувате там, където продуктите и услугите ви са забранени. Google Play може да поиска от вас да предоставите допълнителна информация или документи, които подкрепят това, че спазвате приложимите регулаторни изисквания и тези за лицензиране.

Добив на криптовалUTI

Не допускаме приложения, които добиват криптовалUTI на устройства. Разрешаваме приложения за отдалечено управление на добива на криптовалUTI.

Изисквания за прозрачност за дистрибуцията на заместени с означение дигитални активи

Ако приложението ви продава заместени с означение дигитални активи или дава възможност на потребителите да спечелят такива, трябва да декларирате това чрез формуляра за финансови функции на страницата „Съдържание на приложението“ в Play Console.

Когато създавате продукт в приложение, в подробностите за него трябва да посочите, че представлява заместен с означение дигитален актив. За допълнителни указания разгледайте [Създаване на продукт в приложение](#).

Нямате право да популяризирате или да представяте в привлекателна светлина потенциалните приходи от игра или търгуване.

Допълнителни изисквания за игровизацията чрез NFT

Съгласно изискванията на [правилата на Google Play за хазарт, игри и състезания с истински пари](#) приложенията за хазарт, които интегрират заместени с означение дигитални активи,

като например NFT, трябва да завършат процеса на кандидатстване.

За всички други приложения, които не отговарят на условията за приложенията за хазарт и не са включени в [Пилотни програми за други игри с истински пари](#), нищо с парична стойност не трябва да се приема в замяна на възможността за получаване на NFT с неизвестна стойност. Купените от потребителите NFT трябва да бъдат изразходвани или използвани в играта с цел подобряване на практическата работа или подпомагане на потребителите с напредъка в играта. NFT не трябва да се използват като залог в замяна на възможността да се спечелят награди с реална парична стойност (включително други NFT).

Ето няколко примера за често срещани нарушения:

- Приложения, които продават пакети с NFT, без да разкриват конкретното съдържание и стойност на отделните NFT.
- Социални казино игри, при които се плаща за игра (например ротативки), които дават NFT като награда.

Генерирано от AI съдържание

Моделите с генеративен AI стават все по-достъпни за програмистите и е възможно да въградите такива модели в приложенията си, за да увеличите ангажираността и да подобрите практическата работа на потребителите. Google Play иска да гарантира, че генерираното от AI съдържание е безопасно за всички потребители и че обратната връзка от потребителите се използва за постигане на отговорни иновации.

Генерирано от AI съдържание

Генерираното от AI съдържание е съдържание, създадено от модели на генеративен AI въз основа на подкани от потребителя. Примерите за такова съдържание включват:

- Чатботове с генеративен AI за текстови разговори, при които взаимодействието с чатбота е основна характеристика на приложението
- Изображение, генерирано от AI въз основа на текстови, графични или гласови подкани.

За да се гарантира безопасността на потребителите и в съответствие с [обхвата на правилата](#) на Google Play, приложенията, които генерират съдържание чрез AI, трябва да спазват правилата за програмистите в Google Play, включително като забраняват и не допускат генерирането на [ограничено съдържание](#), като например [съдържание, което улеснява експлоатацията или насилието над деца](#), както и съдържание, което позволява [подвеждащо поведение](#).

Приложенията, които генерират съдържание чрез AI, трябва да съдържат функции за означаване или сигнализиране от потребители в самото приложение, чрез които хората да могат да означават обидно съдържание или да подават сигнали за него до програмистите, без да се налага да излизат от приложението. Програмистите трябва да използват сигналите от потребителите, за да коригират филтрирането на съдържанието и модерират в приложенията.

Интелектуална собственост

Не допускаме приложения или профили на програмисти, които нарушават чужди права на интелектуална собственост (включително патентни и авторски права, права за запазени марки и търговски тайни, както и други права на собственост). Също така не допускаме приложения, които насърчават или подбуждат към нарушаването на права на интелектуална собственост.

Ще отговаряме на ясни известия за предполагаемо нарушаване на авторски права. За повече информация или за да подадете искане съгласно Закона за авторските права в цифровото

хиялолетие (DMCA), прегледайте [процедурите ни относно авторските права](#) .

За да подадете жалба относно продажбата на фалшифицирани стоки или популяризирането им с такава цел в дадено приложение, изпратете [известие относно фалшификация](#) .

Ако смятате, че приложение в Google Play нарушава правата ви за запазена марка, на която сте собственик, препоръчваме ви да се свържете директно с програмиста, за да се справите с проблема. В случай че не успеете да стигнете до решение, подайте жалба за запазена марка чрез този [формуляр](#) .

Ако разполагате с писмена документация, която доказва, че имате разрешение да използвате интелектуална собственост на трета страна в приложението или малката си обява в магазина (напр. търговски наименования, логотипи и графични активи), [свържете се с екипа на Google Play](#) , преди да изпратите приложението си, за да не бъде отхвърлено поради нарушаване на права на интелектуална собственост.

Неупълномощено използване на съдържание, защитено с авторски права

Не допускаме приложения, които нарушават авторски права. Промяната на защитено с авторски права съдържание пак може да доведе до нарушение. Възможно е да поискаме от програмистите да предоставят доказателства за правата си да използват съответното съдържание.

Моля, бъдете внимателни, когато използвате защитено с авторски права съдържание, за да демонстрирате функционалността на приложението си. По принцип най-безопасният подход е да създадете нещо оригинално.

Ето няколко примера за често срещани нарушения:

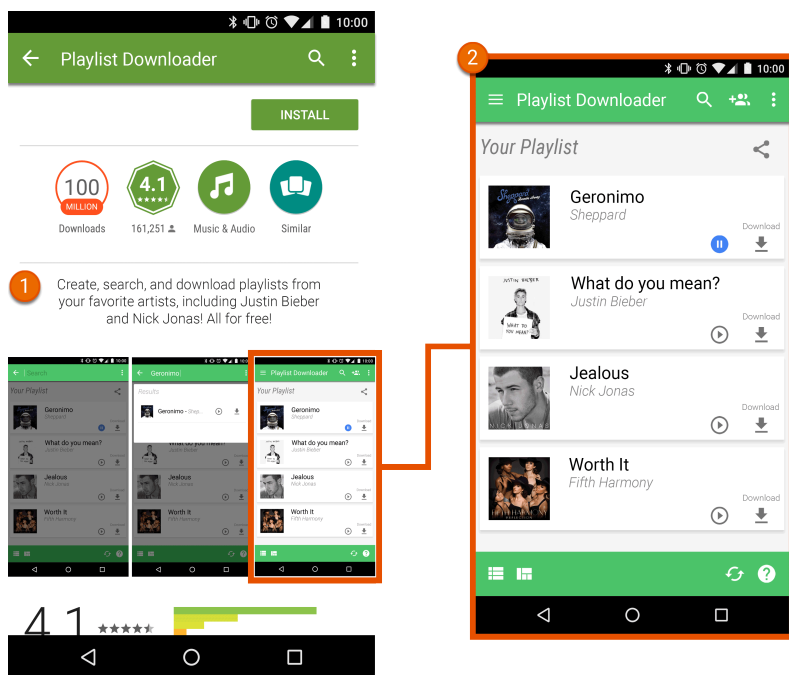
- Обложки на музикални албуми, видеоигри и книги.
- Разпространяване на изображения от филми, телевизионни предавания или видеоигри.
- Илюстрации или изображения от комикси, анимационни и игрални филми, музикални видеоклипове или телевизионни предавания.
- Логотипи на колежански и професионални спортни отбори.
- Снимки, взети от профила на обществена личност в социалните медии.
- Професионални изображения на обществени личности.
- Репродукции или създадени от почитатели произведения, неразличими от защитената с авторски права оригинална творба.
- Приложения със смесителен пулт, който възпроизвежда аудиоклипове от защитено с авторски права съдържание.
- Пълни репродукции или преводи на книги, които не са обществено достояние.

Подтикване към нарушаване на авторски права

Не допускаме приложения, които подбуждат или насърчават към нарушаване на авторски права. Преди да публикувате приложението си, проверете дали по някакъв начин подтиква към такова поведение и при необходимост потърсете правен съвет.

Ето няколко примера за често срещани нарушения:

- Приложения за поточно предаване, които дават възможност на потребителите да изтеглят локално копие на защитено с авторски права съдържание без съответното упълномощаване.
- Приложения, които насърчават потребителите да предават поточно и да изтеглят защитени с авторски права произведения, включително музика и видеоклипове, в нарушение на приложимия закон за авторските права.



- ① Описанието в малката обява в магазина за това приложение насърчава потребителите да изтеглят защитено с авторски права съдържание без съответното упълномощаване.
- ② Екранната снимка в малката обява в магазина за приложението насърчава потребителите да изтеглят защитено с авторски права съдържание без съответното упълномощаване.

Нарушаване на запазена марка

Не допускаме приложения, които нарушават чужди запазени марки. Запазената марка представлява дума, символ или комбинация, които идентифицират източника на стока или услуга. След като се сдобие със запазена марка, собственикът ѝ получава изключителни права върху употребата ѝ по отношение на определени стоки или услуги.

Нарушаването на запазена марка е неуместното или неупълномощено използване на идентична или подобна запазена марка по начин, който вероятно ще предизвика объркване относно източника на продукта. Приложението ви може да бъде спряно, ако ползва запазени марки на друга страна по начин, който е вероятно да причини объркване.

Фалшификация

Не допускаме приложения, които продават фалшифицирани стоки или ги популяризират с такава цел. Фалшифицираните стоки съдържат запазена марка или лого, идентични или по същество неразличими от запазената марка на друго лице. Те наподобяват марковите характеристики на стоката в опит да се представят като истински продукт на собственика на търговската марка.

Поверителност, измама и злоупотреба с устройства

Поели сме ангажимент да защитаваме поверителността на потребителите и да им предоставяме безопасна и сигурна среда. Приложенията, които са измамни, злонамерени или предназначени да злоупотребяват с мрежи, устройства или лични данни или да ги използват неправомерно, са строго забранени.

Потребителски данни

Трябва да има прозрачност в начина, по който боравите с потребителските данни (например информация, събрана от или за потребителя, включително за устройството). Това означава да разкривате достъпа, събирането, използването, обработването и споделянето на потребителски данни от страна на приложението ви и да ги използвате само за оповестените цели, които спазват правилата. Имайте предвид, че обработването на лични и чувствителни потребителски данни е предмет и на допълнителните изисквания в секцията за лични и чувствителни потребителски данни по-долу. Тези изисквания на Google Play допълват изискванията на приложимите закони за поверителност и защита на данните.

Ако сте включили код на трета страна (например SDK) в приложението си, трябва да се уверите, че съответният код, както и практиките на третата страна по отношение на потребителските данни от приложението ви спазват програмните правила за програмистите в Google Play, които включват изисквания за употреба и разкриване на информация. Трябва например да се уверите, че доставчиците ви на SDK не продават лични и чувствителни потребителски данни от приложението ви. Това изискване е в сила независимо дали потребителските данни се прехвърлят след изпращане до сървър, или чрез въграждане на код на трета страна в приложението ви.

Лични и поверителни потребителски данни

Личните и чувствителните потребителски данни включват, без изброяването да е изчерпателно, информация, позволяваща лично идентифициране, финансови данни и такива за плащане, удостоверителна информация, данни от телефонни указатели и за контакти, [местоположение на устройството](#) , данни във връзка с обаждания и SMS съобщения, [данни за здравословното състояние](#) , [данни от Health Connect](#) , данни за други приложения на устройството, данни от микрофона и камерата, както и други чувствителни данни за устройството или за използването. Ако приложението ви обработва лични и чувствителни потребителски данни, трябва:

- да ограничите достъпа, събирането, използването и споделянето на лични и чувствителни потребителски данни, получени чрез приложението, като извършвате тези действия само за функции на приложения и услуги, както и за съобразени с правилата цели според основателните очаквания на потребителя:
 - Приложенията, които разширяват употребата на личните и чувствителните данни до показване на реклами, трябва да спазват [правилата на Google Play за рекламите](#) .
 - Също така при необходимост може да прехвърляте данни към [доставчици на услуги](#) или по други правни причини, като например в отговор на валидно правителствено искане, спазване на приложим закон или като част от обединяване или придобиване при наличие на правно подходящо съобщение за потребителите.
- да боравите с всички лични и чувствителни потребителски данни по сигурен начин, включително да ги предавате посредством съвременни криптографски решения (например през HTTPS).
- при възможност да използвате заявка за разрешения по време на изпълнение, преди да осъществите достъп до данни, ограничени от [разрешения в Android](#) .
- да не продавате личните и чувствителните потребителски данни.
 - „Продажба“ е обменът или прехвърлянето на лични и чувствителни потребителски данни към [трети страни](#) срещу финансова облага.
 - Започнато от потребителя прехвърляне на лични и чувствителни потребителски данни (когато например потребителят използва функция на приложението, за да прехвърли файл към трета страна, или когато той по собствено желание използва специално приложение за научно изследване) не се смята за продажба.

Изискване за разкриване на информация по ясен начин и получаване на съгласие

В случаите, когато достъпът, събирането, използването и споделянето на лични и чувствителни потребителски данни може да са извън основателните очаквания на

потребителя за въпросния продукт или функция (ако например събирането на данни се извършва на заден план, докато потребителят не използва приложението ви), трябва да изпълнявате следните изисквания:

Разкриване на информация по ясен начин: В приложението ви трябва да бъде разкрита информация за достъпа, събирането, използването и споделянето на данни от ваша страна. Разкриването на информация:

- трябва да бъде в самото приложение, а не само в описанието му или на уебсайт;
- трябва да се показва при обичайно използване на приложението, без да се налага потребителят да отваря меню или настройки;
- трябва да описва данните, до които се осъществява достъп или които се събират;
- трябва да обяснява как ще се използват и/или споделят данните;
- не може да се намира само в общи условия или декларация за поверителност;
- не може да бъде включено в други съобщения за разкриване на информация, които не са свързани със събирането на лични и чувствителни потребителски данни.

Съгласие и разрешения за изпълнение: Исканията в приложението за съгласие на потребителя и тези за разрешение за изпълнение трябва непосредствено да бъдат предхождани от съобщение за разкриване на информация в приложението. Това съобщение трябва да отговаря на изискванията на текущите правила. За искането за съгласие трябва да е изпълнено следното:

- диалоговият прозорец за съгласие трябва да бъде представен по ясен и еднозначен начин;
- даването на съгласие трябва да става с изрично действие от страна на потребителя (например докосване, поставяне на отметка в квадратче);
- напускането на съобщението за разкриване на информация (включително напускането чрез докосване отстрани или чрез натискането на бутона за връщане или на бутона „Начало“) не трябва да се тълкува като съгласие;
- за получаването на съгласието на потребителя не трябва да се използват съобщения, които се отхвърлят или затварят автоматично;
- съгласието трябва да бъде предоставено от потребителя, преди приложението ви да започне да събира или да осъществява достъп до личните и чувствителните потребителски данни.

Приложенията, които разчитат на други правни основания, за да обработват лични и чувствителни потребителски данни без съгласие, като например законния интерес съгласно Общия регламент на ЕС относно защитата на данните (ОРЗД), трябва да отговарят на всички приложими правни изисквания и да осигурят на потребителите подходящи съобщения за разкриване на информация, включително в приложението, както се изисква от текущите правила.

С цел спазване на изискванията, свързани с правилата, препоръчително е да следвате следния примерен формат за съобщението за разкриване на информация по ясен начин, когато се изисква такава:

- „[Това приложение] събира/предава/синхронизира/съхранява [тип данни], за да активира [„функция“] [за съответния случай на употреба]“.
- *Пример: „Fitness Funds събира данни за местоположението, за да активира проследяването на физически упражнения дори когато приложението е затворено или не се използва. То се ползва и за поддържане на рекламирането.“*
- *Пример: „Call buddy събира, чете и записва данните от списъка с обажданията, за да активира връзката с организацията дори когато приложението не се използва.“*

Ако в приложението ви е интегриран код на трета страна (например SDK), чието стандартно предназначение е да събира лични и чувствителни потребителски данни, в рамките на 2 седмици от получаването на искане от Google Play (или в рамките на по-дълъг

период от време, ако е посочен такъв в искането от Google Play) трябва да предоставите достатъчно доказателства в подкрепа на това, че приложението ви спазва изискванията, свързани с текущите правила, за разкриване на информация по ясен начин и получаване на съгласие, включително по отношение на достъпа, събирането, използването и споделянето на данни посредством кода на трета страна.

Ето няколко примера за често срещани нарушения:

- Приложение събира местоположението на устройството, но не съдържа съобщение за разкриване на информация по ясен начин, в което се обяснява коя функция използва данните и/или употребата на приложението на заден план;
- Приложение има разрешение за изпълнение, с което заявява достъп до данни преди съобщението за разкриване на информация по ясен начин, в което се посочва за какво се използват.
- Приложение чете данните за инсталираните приложения на потребителя, но не ги третира като лични или поверителни данни, предмет на горепосочените изисквания за декларация за поверителност, обработване на данни, разкриване по явен начин и получаване на съгласие;
- Приложение чете данните от телефонния указател или указателя с контакти на потребителя, но не ги третира като лични или поверителни данни, предмет на горепосочените изисквания за декларация за поверителност, обработване на данни, разкриване по явен начин и получаване на съгласие;
- Приложение, което записва екрана на потребителя, не третира съответните данни като лични или поверителни съгласно тези правила;
- Приложение, което събира [данни за местоположението на устройството](#) и не разкрива изчерпателно използването им и не получава съгласие в съответствие с горепосочените изисквания.
- Приложение, което използва ограничени разрешения на заден план, включително за проследяване, проучване или маркетингови цели, не разкрива изчерпателно начина, по който се използва, и не получава съгласие в съответствие с горепосочените изисквания.
- Приложение с SDK, който събира лични и чувствителни потребителски данни и не ги третира като предмет на текущите правила за потребителските данни и на изискванията, свързани с достъпа и обработването на данните (включително неопозволената продажба), и тези за разкриване на информация по ясен начин и получаване на съгласие.

За повече информация относно изискването за разкриване на информация по ясен начин и получаване на съгласие вижте тази [статия](#).

Ограничения за достъп до личните и поверителните данни

В таблицата по-долу са описани допълнителните изисквания за конкретни дейности.

Дейност	Изискване
Приложението ви борава с финансова информация, данни за плащане или държавни идентификационни номера	То не бива да разкрива обществено лични и поверителни потребителски данни, свързани с финансови или платежни дейности, нито държавни идентификационни номера.
Приложението ви борава с данни от телефонни указатели или информация за връзка, които не са публични	Не разрешаваме неупълномощеното публикуване или разкриване на контакти на потребителя, които не са общодостъпни.
Приложението ви съдържа антивирусна или защитна функционалност, например функции за борба срещу вируси/злонамерен софтуер или такива, свързани със сигурността	То трябва да има декларация за поверителност, която заедно с разкриванията на информация в него посочва какви потребителски данни се събират и предават, как се използват и с какви типове страни се споделят.

Приложението ви е насочено към деца	То не трябва да включва SDK, които не са одобрени за използване в насочени към деца услуги. За пълните правила и изисквания прегледайте страницата Създаване на приложения за деца и семейства .
Приложението ви събира постоянни идентификатори на устройството или прави връзки с тях (напр. IMEI, IMSI, серийния номер на SIM картата и др.)	Постоянните идентификатори на устройството не бива да се свързват с други лични и поверителни потребителски данни или идентификатори на устройства, които могат да бъдат нулирани, освен за следните цели: • телефонни услуги, свързани с конкретна SIM карта (напр. обаждания през Wi-Fi, свързани с профил към оператор); • приложения за управление на корпоративно устройство, които използват режима за собственик на устройството. Тези начини на използване трябва да бъдат представени на потребителите по ясен начин, както е описано в правилата за потребителските данни. За алтернативните уникални идентификатори прегледайте този ресурс. За допълнителни указания относно идентификатора за рекламиране за Android прочетете правилата за рекламите.

Секция за безопасност на данните

Всички програмисти трябва да попълнят ясно и точно секцията за безопасност на данните за всяко приложение, като предоставят информация относно събирането, използването и споделянето на потребителски данни. Програмистите носят отговорност за точността на етикета за поверителността и актуализирането на тези данни. Където е уместно, информацията в секцията трябва да съответства на разкриванията в декларацията за поверителност на приложението.

Направете справка с [тази статия](#) за допълнителна информация относно попълването на секцията за безопасност на данните.

Декларация за поверителност

Трябва да публикувате връзка към декларация за поверителност за всички приложения в предназначенията за целта поле в Play Console, а в самото приложение – текста на декларацията или връзка към нея. Декларацията за поверителност трябва, заедно с разкриванията на информация в приложението, изчерпателно да описва начина, по който приложението осъществява достъп до потребителските данни, как ги събира, използва и споделя. Това не се отнася само за данните, описани в секцията за безопасност на данните. Декларацията трябва да съдържа:

- информация за програмиста и данни за връзка или механизъм за изпращане на запитвания, свързани с поверителността;
- разкриване на типовете лични и поверителни потребителски данни, до които приложението ви осъществява достъп и които събира, използва и споделя, както и страните, с които се споделят такива данни;
- сигурни процедури за обработване на личните и поверителните потребителски данни;
- правилата на програмиста относно запазването и изтриването на данни;
- ясно обозначаване като „декларация за поверителност“ (например в заглавието).

Декларацията за поверителност трябва да съдържа името на приложението или на юридическото лице (например програмист или дружество), посочено в малката обява на

приложението в Google Play Магазин. Приложенията, които не осъществяват достъп до лични и поверителни потребителски данни, също трябва да изпратят декларация за поверителност.

Тя трябва да е публикувана на активен обществено достъпен URL адрес без геозониране (не във формат PDF) и да е без възможност за редактиране.

Изискване за изтриване на профила

Ако потребителите имат възможност да създават профили в приложението ви, тогава те трябва да могат да правят заявки за изтриване на съответните профили от самото приложение. Потребителите трябва да разполагат с лесно откриваема опция за стартиране на изтриването на профила в приложението и извън него (например като посетят уебсайта ви). Връзка към този уеб ресурс трябва да бъде въведена в определеното поле за URL адрес на формуляра в Play Console.

Когато изтриете даден профил в приложение въз основа на заявка от потребителя, трябва да изтриете и потребителските данни, свързани със съответния профил. Временното изключване, деактивирането или „замразяването“ на профила в приложението не се считат за изтриване на профила. Ако се налага да запазите определени данни поради законни причини, като например с цел сигурност, предотвратяване на измами или спазване на нормативни изисквания, трябва ясно да информирате потребителите за практиките си за запазване на данни (например в декларацията си за поверителност).

За да научите повече за изискванията на правилата относно изтриването на профила, прегледайте тази статия в [Помощния център](#). За допълнителна информация относно актуализирането на формуляра за безопасност на данните вижте [тази статия](#).

Използване на идентификатора за настройки на приложението

В Android ще бъде въведен нов идентификатор за поддържане на най-важните случаи на употреба, като например анализ и предотвратяване на измами. Следват условията за употребата на този идентификатор.

- **Употреба:** ID на набора приложения не трябва да се използва за персонализиране и измерване на рекламите.
- **Свързване с информация, позволяваща лично идентифициране, или други идентификатори:** ID на набора приложения не трябва да бъде свързан с други идентификатори за Android (напр. идентификатора за рекламиране за Android), нито с лични и чувствителни данни за рекламни цели.
- **Прозрачност и съгласие:** Извличането и използването на ID на набора приложения, както и обвързването с тези условия трябва да бъдат разкрити на потребителите в юридически издържано съобщение за поверителност, включително в декларацията ви за поверителност. Трябва да получите юридически валидно съгласие от потребителите, когато това е задължително. За да научите повече за стандартите ни за поверителност, прегледайте [правилата ни за потребителските данни](#).

EU-U.S., Swiss Privacy Shield (Щит за личните данни в отношенията между ЕС и САЩ и Швейцария и САЩ)

Ако осъществявате достъп, използвате или обработвате лична информация, предоставена от Google, която пряко или непряко идентифицира човек и която произлиза от Европейския съюз или Швейцария („Лична информация от ЕС“), трябва:

- да спазвате всички приложими закони, директиви, разпоредби и правила относно поверителността и относно защитата и сигурността на данните;
- да осъществявате достъп до, използвате или обработвате лична информация от ЕС само за целите, за които е дал съгласието си човекът, за когото се отнася тази информация;

- да внедрите подходящи организационни и технически мерки за защитата на личната информация от ЕС от загуба, злоупотреба и неупълномощен или незаконен достъп, разкриване, промяна и унищожаване;
- да осигурите нивото на защита, което се изисква съгласно [принципите на Privacy Shield](#) .

Трябва постоянно да следите дали спазвате тези условия. Ако в някой момент не можете да ги изпълните (или има значителен риск да не можете да ги изпълните), трябва незабавно да ни известите с имейл до адрес data-protection-office@google.com и веднага да престанете да обработвате лична информация от ЕС или да предприемете подходящи и разумни действия за възстановяване на адекватно ниво на защита.

От 16 юли 2020 г. Google вече не разчита на EU-U.S. Privacy Shield за предаването на лични данни от Европейското икономическо пространство или Обединеното кралство към САЩ. ([Научете повече.](#)) Повече информация е посочена в раздел 9 на DDA.

Разрешения и API, които осъществяват достъп до поверителна информация

Исканията за разрешения и използване на API, които осъществяват достъп до поверителна информация, трябва да са разбираеми за потребителите. Може да искате само разрешения и да ползвате API с достъп до поверителна информация, когато това е необходимо за реализирането на текущи функции или услуги в приложението ви, посочени в малката обява за него в Google Play. Не може да използвате разрешения и API с достъп до поверителна информация, които дават достъп до потребителски данни или такива за устройството, за неразкрити, нереализирани или забранени функции или цели. Забранено е лични или чувствителни данни, получени чрез тези разрешения или API, да се продават или споделят с цел улесняване на продажбата им.

Ползвайте API с достъп до поверителна информация и искайте разрешения за достъп до данни в контекст (чрез постепенно увеличаване), така че потребителите да разбират защо е нужно това. Използвайте данните само за целите, за които потребителят е дал съгласието си. Ако впоследствие пожелаете да използвате данните за други цели, трябва да попитате потребителите и да получите съгласието им за допълнителната употреба.

Ограничени разрешения

В допълнение към по-горното ограничениите разрешения са такива, които са обозначени като [Dangerous](#) , [Special](#) , [Signature](#) или по долупосочените начини. Тези разрешения са предмет на следните допълнителни изисквания и ограничения:

- Потребителски данни и такива за устройството, до които е осъществен достъп посредством ограничени разрешения, се смятат за лични и чувствителни потребителски данни. В сила са изискванията, свързани с [правилата за потребителските данни](#) .
- Уважавайте решенията на потребителите, ако отхвърлят искане за ограничено разрешение. Потребителите не бива да бъдат манипулирани или принуждавани да се съгласят да предоставят което и да било некритично разрешение. Трябва да положите разумни усилия да осигурите работата на потребителите, които не предоставят разрешения за достъп до поверителна информация (например като разрешите на потребителя ръчно да въведе телефонен номер, ако е ограничил достъпа до списъка с обажданията).
- Използването на разрешения в разрез с [правилата на Google Play относно злонамерения софтуер](#) (включително [тези за злоупотреба с администраторски права](#)) е изрично забранено.

Някои ограничени разрешения може да са предмет на допълнителни изисквания, както е описано по-долу. Целта на тези ограничения е да се предпази поверителността на

потребителите. Възможно е да направим изключения от посочените по-долу изисквания в много редки случаи, когато приложенията предоставят изключително наложителна или критична функция и няма алтернативен метод за осигуряването ѝ. За предложените изключения преценяваме потенциалното въздействие върху поверителността и сигурността на потребителите.

Разрешения за достъп до SMS и списъка с обажданията

Разрешенията за достъп до SMS и списъка с обажданията се считат за лични и поверителни потребителски данни, които са предмет на правилата за [личната и поверителната информация](#) и следните ограничения:

Ограничено разрешение

Група разрешения, свързани със списъка с обажданията (напр. READ_CALL_LOG, WRITE_CALL_LOG, PROCESS_OUTGOING_CALLS)

Група разрешения за SMS съобщения (напр. READ_SMS, SEND_SMS, WRITE_SMS, RECEIVE_SMS, RECEIVE_WAP_PUSH, RECEIVE_MMS)

Изискване

Приложението трябва да е активно регистрирано като стандартния телефонен манипулатор или такъв за асистент в устройството.

Приложението трябва да е активно регистрирано като стандартния манипулатор за SMS съобщения или за асистент в устройството.

Използването на горепосочените разрешения не може да се декларира в манифеста на приложения, които не са в състояние да бъдат стандартният манипулатор за телефонни обаждания, за SMS съобщения или за асистент. Това включва заместващия текст в манифеста. Също така приложенията трябва да са активно регистрирани като стандартния манипулатор за телефонни обаждания, за SMS съобщения или за асистент, преди да подканят потребителите да приемат което и да е от горепосочените разрешения. Те трябва незабавно да спрат да използват разрешението, след като престанат да бъдат стандартният манипулатор. Разрешенията начини на ползване и изключенията са публикувани на [тази страница в Помощния център](#).

Приложенията може да използват съответното разрешение (и получените чрез него данни) само за осигуряване на одобрена основна функционалност. Основната функционалност е главното предназначение на приложението. Тя може да включва набор от основни функции, които трябва да са ясно документираны и представени в описанието му. Без тези функции приложението няма да работи правилно или ще бъде неизползваемо. Прехвърлянето, споделянето или лицензираното използване на тези данни трябва да служи само за осигуряване на основни функции или услуги в приложението. Използването на данните за други цели (напр. за подобряване на други приложения или услуги, за рекламиране или маркетинг) е забранено. Не може да използвате алтернативни методи (включително други разрешения, приложни програмни интерфейси (API) или източници на трети страни) за получаване на данни, свързани с разрешенията за достъп до SMS или списъка с обажданията.

Разрешения за достъп до местоположението

[Местоположението на устройството](#) се счита за лични и поверителни потребителски данни, които са предмет на правилата за [личната и поверителната информация](#), [правилата за местоположението на заген план](#) и следните изисквания:

- Приложенията нямат право да осъществяват достъп до данни, защитени от разрешения за местоположението (напр. ACCESS_FINE_LOCATION, ACCESS_COARSE_LOCATION, ACCESS_BACKGROUND_LOCATION), след като те повече не са необходими за осигуряване на текущи функции или услуги в съответното приложение.
- Никога не бива да искате от потребителите разрешения за местоположение единствено с цел реклама или анализ. Приложенията, които разширяват разрешената употреба на тези

данни, за да показват реклами, трябва да спазват [правилата ни за рекламите](#) .

- Приложенията трябва да искат най-малкия обхват на достъп до местоположението (т.е. с ниска вместо с висока точност и на преден вместо на заден план), необходим за осигуряване на текущата функция или услуга, която иска това, а потребителите трябва с основание да очакват, че функцията или услугата се нуждае от заявеното ниво на достъп. Например може да отхвърлим приложения, които искат или осъществяват достъп до местоположението на заден план без убедителна обосновка.
- Достъпът до местоположението на заден план може да се използва само за предоставяне на полезни за потребителя функции, свързани с основната функционалност на приложението.

На приложенията е разрешено да осъществяват достъп до данни за местоположението, като ползват разрешението за услуга на преден план (когато приложението има само достъп на преден план, напр. докато се използва), ако употребата:

- е продължение на действие, започнато от потребителя; и
- се прекратява незабавно, след като действието, започнато от потребителя, бъде изпълнено от приложението.

Приложенията, създадени специално за деца, трябва да спазват правилата на програмата [Приложения за семейството](#) .

За повече информация относно изискванията на правилата разгледайте [тази помощна статия](#) .

Разрешение за достъп до всички файлове

Файловете и атрибутите в директориите на устройството на потребителя се считат за лични и поверителни потребителски данни, които са предмет на правилата за [личната и поверителната информация](#) и следните изисквания:

- Приложенията трябва да искат достъп до хранилището на устройството само ако е от решаващо значение за функционирането им, и нямат право да искат такъв достъп от името на трета страна за цели, които не са свързани със съществена функция, насочена към потребителя.
- Устройствата с Android R или по-нова версия ще трябва да имат разрешението [MANAGE_EXTERNAL_STORAGE](#) , за да управляват достъпа до споделеното хранилище. Всички приложения, които са предназначени за Android R и изискват обширен достъп до споделеното хранилище („Достъп до всички файлове“), трябва да преминат успешно съответната проверка на достъпа, преди да бъдат публикувани. Приложенията, на които е позволено да използват това разрешение, трябва ясно да подканват потребителите да разрешат достъпа до всички файлове за приложението от секцията с настройки „Специален достъп за приложението“. За повече информация относно изискванията за Android R, моля, разгледайте тази [помощна статия](#) .

Разрешение за видимостта на пакетите (приложенията)

Информацията за инсталираните приложения, прочетена от гадено устройство, се счита за лични и поверителни потребителски данни, които са предмет на правилата [за личната и поверителната информация](#) и на следните изисквания:

Приложенията, чиято основна цел е да стартират, търсят или взаимодействат с други приложения на устройството, може да получат видимост със съответния обхват за другите инсталирани приложения на устройството, както е посочено по-долу:

- **Широка видимост на приложенията:** Това е възможността гадено приложение да има голяма (или „широка“) видимост за инсталираните приложения („пакети“) на устройството.

- За приложения, които са насочени към [30-о или по-високо ниво на API](#) , широката видимост на инсталираните приложения чрез разрешението [QUERY_ALL_PACKAGES](#) е ограничена до конкретни случаи на употреба, при които информираността за и/или съвместимостта с някои или всички приложения на устройството са необходими за функционирането на приложението.
- Приложението ви не бива да използва [QUERY_ALL_PACKAGES](#), ако може да работи с [декларация за видимостта на пакетите с по-тесен обхват](#) (напр. запитване към и взаимодействие с конкретни пакети, вместо да се иска широка видимост).
- Използването на алтернативни методи за постигане на поведение, близко до широкото ниво на видимост, свързано с разрешението [QUERY_ALL_PACKAGES](#), също е ограничено до основната функционалност на приложението, насочена към потребителя, и съвместимостта с приложенията, открити чрез този метод.
- За допустимите случаи на употреба за разрешението [QUERY_ALL_PACKAGES](#), моля, разгледайте тази [статия в Помощния център](#) .
- **Ограничена видимост на приложенията:** Такава видимост има, когато приложението свежда до минимум достъпа до данни, като прави заявки за конкретни приложения посредством по-насочени (вместо „широки“) методи (напр. чрез заявки за конкретни приложения, които съответстват на декларацията в манифеста на приложението ви). Може да използвате този метод за изпращане на заявки за приложения в случаите, когато съвместимостта на приложението ви отговаря на правилата, както и за управление на тези приложения.
- Видимостта на рекламните места на инсталираните приложения на устройството трябва да е пряко свързана с основната цел или основната функционалност, до които потребителите имат достъп в рамките на приложението ви.

Данните за приложенията, получени от разпространявани чрез Google Play приложения, е забранено да се продават, както и да се споделят с цел анализ или осигуряване на приходи от реклами.

API за достъпност

Не е разрешено използването на API за достъпност с цел:

- промяна на потребителските настройки без съответното разрешение или възпрепятстване на способността на потребителите да деактивират или деинсталират дадено приложение или услуга, освен ако това не е разрешено от родител или настойник чрез приложение за родителски контрол или от упълномощен администратор посредством софтуер за корпоративно управление;
- заобикаляне на вградените в Android контроли и известия за поверителност;
- промяна или използване на потребителския интерфейс по подвеждащ начин или по друг начин, нарушаващ правилата за програмисти в Google Play.

API за достъпност не е предназначен и не може да бъде изискван за аудиозапис на другата страна в обажданията.

Използването на API за достъпност трябва да бъде документирано в малката обява в Google Play.

Указания за `IsAccessibilityTool`

Приложенията, чиято основна функционалност има за цел директно да помага на хора с увреждания, отговарят на условията за използване на маркера `IsAccessibilityTool`, за да бъдат представяни правилно в публичното пространство като приложения за достъпност.

Тези, които не отговарят на условията за ползване на `IsAccessibilityTool`, нямат право да използват означението и трябва да спазват изискванията за разкриване и получаване на съгласие по ясен начин, които са описани в [правилата за потребителските данни](#) , тъй

като свързаната с достъпността функционалност не е очевидна за потребителя. За повече информация вижте статията в Помощния център за [API на AccessibilityService](#).

Когато е възможно, приложенията трябва да използват [API и разрешения](#) с по-ограничен обхват вместо API за достъпност, за да осигурят желаната функционалност.

Заявяване на разрешение за инсталиране на пакети

Разрешението [REQUEST_INSTALL_PACKAGES](#) дава възможност на гадено приложение да заявява инсталирането на пакети на приложения. За да използвате това разрешение, основната функционалност на приложението ви трябва да включва:

- изпращане или получаване на пакети на приложения;
- даване на възможност на потребителя да инициира инсталиране на пакети на приложения.

Разрешените функционалности включват:

- сърфиране в мрежата или търсене;
- услуги за комуникация, които поддържат прикачени файлове;
- споделяне, прехвърляне или управление на файлове;
- управление на корпоративно устройство;
- резервни копия и възстановяване;
- мигриране на устройството/прехвърляне на телефона;
- придружаващо приложение за синхронизиране на телефона с носим аксесоар или с устройство в ИИ (например смартчасовник или смарттелевизор).

Основната функционалност е главното предназначение на приложението. Основната функционалност, както и всички основни функции, които тя включва, трябва да бъдат ясно документираны и представени в описанието на приложението.

Разрешението REQUEST_INSTALL_PACKAGES не може да се използва за извършване на самоактуализации, промени или групиране на други APK във файла на актива освен с цел управление на устройството. Всички актуализации или инсталирания на пакети трябва да спазват [правилата на Google Play относно злоупотреба с устройства и мрежи](#) и да бъдат започнати и извършени от потребителя.

Разрешения за Health Connect от Android

[Health Connect](#) е платформа под Android, която позволява на приложенията за здраве и физическа активност да съхраняват и споделят едни и същи локални данни в единна екосистема. Също така платформата осигурява централизирано място, от което потребителите да управляват възможността на приложенията да четат и записват данни за здравето и физическата активност, включително здравни картони. Здравните картони може да включват медицинска история, диагнози, лечения, лекарства, лабораторни резултати и други клинични данни, получени от доставчици на здравни грижи или здравни институции, или чрез поддържани здравни платформи на трети страни.

Health Connect поддържа четенето и записването на [различни типове данни](#) – от крачки и телесна температура до данни в здравни картони.

Данните, достъпни чрез разрешенията за Health Connect, се смятат за лични и поверителни потребителски данни, които са предмет на [правилата за потребителските данни](#). Ако приложението ви отговаря на изискванията за здравно приложение или има функции, свързани със здравето, и достъп до данни за здравословното състояние, включително данни от Health Connect, то трябва да спазва и [правилата относно приложенията за здраве](#).

За информация как да започнете да използвате Health Connect, вижте това [ръководство за програмисти за Android](#). За да заявите достъп до типове данни в Health Connect и да

разгледайте други често задавани въпроси, вижте [Често задавани въпроси за изискванията на правилата за Health Connect](#).

За да четат и/или записват данни в Health Connect, разпространяваните чрез Google Play приложения трябва да отговарят на следните изисквания на правилата.

Достъп до и използване на Health Connect за подходящи цели

Health Connect може да се използва само в съответствие с приложимите правила и Общи условия и за одобрените случаи на употреба, посочени в настоящите правила. Това означава, че имате право да заявите достъп до разрешения само ако приложението или услугата ви ги изискват за някой от одобрените случаи на употреба.

Одобрените случаи на употреба включват: физическа активност и благосъстояние, награди, фитнес обучение с инструктор, уелнес за фирми, медицински грижи, проучвания, свързани със здравето, и игри. Приложенията, на които е даден достъп за тези случаи на употреба, нямат право да разширяват употребата на Health Connect до неразкрити или невалидни цели.

Достъп до разрешенията за Health Connect може да се заявява само за приложенията или услугите с една или повече функции, чиято цел е подобряване на здравето и физическата форма на потребителите. Те включват:

- приложения или услуги, които дават възможност на потребителите **директно да записват, отчитат, наблюдават и/или анализират** физическата активност, съня, психичното благополучие, храненето, здравните показатели, описанията на физическото състояние, здравните картони и/или други описания и измервания, свързани със здравето или физическата форма;
- приложения или услуги, които дават възможност на потребителите **да съхраняват на устройството си данни за физическата активност, съня, психичното благополучие, храненето, здравните показатели, описанията на физическото състояние, здравните картони** и/или други описания и измервания, свързани със здравето или физическата форма, както и да споделят данните си с други приложения на устройството, подходящи за тези случаи на употреба;
- приложения или услуги, които дават възможност на потребителите да управляват хронични състояния, медицински лечения или грижи.

Достъпът до Health Connect не може да бъде използван в нарушение на настоящите правила или на другите приложими Общи условия и правила на Health Connect, включително за следните цели:

- Използване на Health Connect за разработване на или включване в приложения, среди или активности, при които може основателно да се очаква използването или неправилното функциониране на Health Connect да доведат до смърт, нараняване, вреда за хората, замърсяване на околната среда или имуществена вреда (например създаване или управление на ядрени съоръжения, системи за контрол на въздушния трафик, животоподдържащи системи или оръжия).
- Достъп до данните, получени чрез Health Connect, посредством приложения без графичен потребителски интерфейс. Приложенията трябва да имат икона, която ясно ги идентифицира и се показва в областта с приложенията, настройките за приложенията на устройството, иконите за известия и гр.
- Използване на Health Connect с приложения, които синхронизират данни между несъвместими устройства или платформи.
- Използване на Health Connect за свързване с приложения, услуги или функции, които са насочени само към деца.
- Предприемете разумни и подходящи стъпки, за да защитите всички приложения или системи, които използват Health Connect, от неупълномощен или незаконен достъп, използване, унищожаване, загуба, промяна или разкриване на информация.

Ваше задължение е също така да спазвате всички нормативни или законови изисквания, които може да са в сила въз основа на целта, за която използвате платформата Health Connect и данни от нея. Ако например сте обхванато лице или бизнес партньор, които са предмет на Закона на САЩ за приемственост и отчетност на здравето осигуряване (HIPAA), трябва да спазвате приложимите изисквания за осъществяването на достъп до и използването на информация от Health Connect от ваша страна. Ако сте програмист, който е предмет на Общия регламент относно защитата на данните (ОРЗД) за потребителите в ЕС, също така трябва да спазвате задълженията си съгласно ОРЗД. Тези закони и разпоредби може да изискват да сключите допълнителни споразумения (напр. споразумение за бизнес съдружие или споразумение за обработване на данни) с приложимите лица, които участват в дейностите ви по обработване. Програмистите на приложения също така носят отговорност да определят дали дейностите им изискват такива споразумения. При поискване програмистите трябва да предоставят на Google доказателства за съответното споразумение или за спазването на изискванията.

Освен ако това не е оповестено изрично в етикетите или информацията от Google за конкретни наши продукти или услуги, Google не дава гаранции за точността на данните в Health Connect и не подкрепя използването им за каквото и да е предназначение или цел и по-специално, използване за изследователски, здравни или медицински цели. Google не поема никаква отговорност във връзка с използването на данните, получени чрез Health Connect.

Ограничено използване

Когато ползвате Health Connect, при осъществяване на достъп и използване на данните трябва да се спазват определени ограничения:

- Използването на данните трябва да бъде ограничено до обезпечаване или подобряване на подходящия случай на употреба или функциите, видими в потребителския интерфейс на приложението.
- Потребителските данни могат да се предават към трети страни само ако потребителят е дал изрично съгласие: във връзка със съображения за сигурност (например за проучване на злоупотреба), за спазване на приложимите закони или регламенти или като част от обединявания/придобивания.
- Достъпът на хора до потребителските данни е ограничен, освен ако потребителят не е дал изрично съгласие, и е възможен само от съображения за сигурност, с цел спазване на законите или когато данните са обобщени за вътрешни цели в съответствие със законовите изисквания.
- **Всички други случаи на предаване, употреба и продажба на данни от Health Connect са забранени, включително:**
 - предаване или продажба на потребителски данни на трети страни, като например рекламни платформи, брокери на данни или дистрибутори на информация;
 - предаване, продажба или използване на потребителски данни с цел показване на реклами, включително персонализирани или въз основа на интереси;
 - предаване, продажба или използване на потребителски данни с цел определяне на кредитоспособността или отпускане на заем;
 - предаване, продажба или използване на потребителски данни с продукт или услуга, които може да бъдат квалифицирани като медицинско устройство, освен ако приложението за медицинското устройство не отговаря на всички приложими разпоредби, включително получаване на необходимите разрешения или одобрения от съответните регулаторни органи (напр. FDA в САЩ) за целите, за които то ще използва данните от Health Connect, и ако потребителят е предоставил изрично съгласие за съответното използване;
 - предаване, продажба или използване на потребителски данни за всякакви цели и по всякакви начини, включващи защитена здравна информация (според определението на HIPAA), освен ако са стартирани от потребителя и спазват изискванията в разпоредбите на HIPAA.

Минимален обхват

Трябва да заявите достъп само до разрешенията, които са необходими за внедряването на функциите или услугите на продукта ви. Съответните заявки за достъп трябва да са конкретни и ограничени до необходимите данни.

Прозрачно и точно известие и контрол

Health Connect обработва данни за здравето и физическата активност, които включват лична и поверителна информация. Програмистите трябва да разкрият практиките си за данни по ясен начин и в достъпен вид чрез изчерпателна декларация за поверителност. Разкриването на информация трябва да включва:

- точно представяне на идентичността на приложението или услугата, които искат достъп до потребителски данни.
- ясна и точна информация, обясняваща типовете данни, до които се осъществява достъп, които се заявяват и/или събират. Данните трябва да бъдат свързани с видима за потребителите функция или препоръка, предлагана в приложението ви.
- обяснение за това как ще се използват и/или споделят данните: ако искате достъп до данните по една причина, но те ще се използват и за друга цел, трябва да разкриете на потребителите всички случаи на употреба.
- помощна документация, която обяснява как потребителите могат да управляват и изтрият данните си от приложението и какво се случва с тях, когато гаген профил бъде деактивиран и/или изтрият.
- информация относно обработването на всички лични и чувствителни потребителски данни по сигурен начин, включително предаването им посредством съвременни криптографски решения (например през HTTPS).

За повече информация относно изискванията за приложения, които се свързват с Health Connect, вижте тази статия в [Помощния център](#).

VPNService

[VpnService](#) е базов клас, който приложенията да разширяват и така да създават свои собствени VPN решения. Само приложенията, които използват VpnService и при които VPN е основна функционалност, могат да създават надежден тунел на ниво устройство към отдалечен сървър. Изключенията се отнасят за приложения, които изискват отдалечен сървър за основната си функционалност, като например:

- приложения за родителски контрол и корпоративно управление;
- проследяване на употребата на приложенията;
- приложения за сигурност на устройството (например антивирусни, за управление на мобилно устройство и за защитна стена);
- инструменти, свързани с мрежи (например отдалечен достъп);
- приложения за сърфиране в мрежата;
- приложения на оператори, за които се изисква използването на VPN с цел предоставяне на услуги за телефония или свързаност.

VpnService не може да се използва за:

- събиране на лични и поверителни потребителски данни без разкриване на информация за това по ясен начин и получаване на съгласие;
- пренасочване или манипулиране на потребителския трафик от други приложения на устройството с цел осигуряване на приходи (например пренасочване на рекламния трафик през държава, която е различна от тази на потребителя);

Приложенията, които използват VpnService, трябва:

- да документират използването на VpnService в малката обява в Google Play;
- да шифроват данните от устройството към крайната точка на VPN тунела;
- да спазват всички [програшни правила за програмистите](#) , включително тези относно [измамите с реклами](#) , [разрешенията](#) и [злонамерения софтуер](#) .

Разрешение за точен будилник

Ще бъде въведено ново разрешение – USE_EXACT_ALARM, което ще дава достъп до [функционалността за точен будилник](#) в приложенията на устройства с Android 13 (целево ниво на API 33).

USE_EXACT_ALARM е ограничено разрешение и приложенията трябва да го декларират само ако основната им функционалност поддържа необходимостта за точен будилник.

Приложенията, които заявяват това ограничено разрешение, подлежат на преглед, а тези, които не отговарят на критериите за приемливи случаи на употреба, няма да могат да бъдат публикувани в Google Play.

Приемливи случаи на употреба за използване на разрешението за точен будилник

Приложението ви трябва да използва функционалността USE_EXACT_ALARM само когато основната му насочена към потребителите функционалност изисква действия, свързани с точен момент, като например:

- Приложението е будилник или таймер.
- Приложението е календар, който показва известия за събития.

Ако вашият случай на употреба за функционалността за точен будилник не е сред описаните по-горе, трябва да прецените дали вместо това е възможно да използвате SCHEDULE_EXACT_ALARM.

За повече информация относно функционалността за точен будилник разгледайте тези [указания за програмисти](#) .

Разрешение за намерение за цял екран

Когато приложенията са насочени към Android 14 (целево ниво на API 34) и по-нови версии, [USE_FULL_SCREEN_INTENT](#) представлява [разрешение за специален достъп за приложението](#) . На приложенията автоматично ще се позволява да използват разрешението USE_FULL_SCREEN_INTENT само ако основната им функционалност е от една от следните категории, за които са необходими известия с висок приоритет:

- задаване на аларма;
- получаване на телефонни или видеообаждания.

Приложенията, които заявяват това разрешение, подлежат на преглед и ако не изпълняват горепосочените критерии, няма автоматично да получат разрешението. В този случай те трябва да искат от потребителя разрешение да използват USE_FULL_SCREEN_INTENT.

Напомняме, че използването на разрешението USE_FULL_SCREEN_INTENT трябва да спазва всички [Правила за програмистите в Google Play](#), включително правилата ни относно [нежелан софтуер за мобилни устройства](#), [злоупотреба с устройства и мрежи](#) и [реклами](#). Известията от намерение на цял екран не могат да осъществяват достъп до устройството на потребителя по неупълномощен начин, нито да пречат на работата му или да я смущават, нито да го повреждат. Също така приложенията не трябва да пречат на други приложения, нито на използваемостта на устройството.

Научете повече за разрешението USE_FULL_SCREEN_INTENT в [Помощния ни център](#).

Злоупотреба с устройства и мрежи

Не допускаме приложения, които могат да повредят, да възпрепятстват или влошат работата на или да осъществяват неупълномощен достъп до устройството на потребителя, други устройства или компютри, сървъри, мрежи, приложни програмни интерфейси (API) или услуги, включително, но не само, други приложения на устройството, която и да е услуга на Google или мрежата на оторизиран оператор.

Приложенията в Google Play трябва да спазват стандартните изисквания за оптимизиране за системата Android, описани в [съответните основни указания за качество](#).

Разпространяваните чрез Google Play приложения не може да променят, заменят или актуализират себе си посредством метод, различен от предлагания от услугата механизъм за актуализиране. Също така приложенията нямат право да изтеглят изпълним код (напр. dex, JAR, .so файлове) от източник, различен от Google Play. Това ограничение не се отнася за кода, който се изпълнява във виртуална машина или интерпретатор, които осигуряват непряк достъп до API на Android (като например JavaScript в WebView или в браузър).

Приложения или код на трета страна (напр. SDK), съдържащи интерпретируеми езици (JavaScript, Python, Lua и др.), които се зареждат по време на изпълнение (напр. такива, които не са пакетирани с приложението), не трябва да допускат потенциални нарушения на правилата на Google Play.

Не допускаме код, който въвежда или използва уязвимости в сигурността. Разгледайте [програмата за подобряване на сигурността на приложенията](#), за да научите повече за най-скорошните проблеми със сигурността, за които е подаден сигнал до програмистите.

Ето няколко примера за често срещани нарушения:

Примери за чести нарушения, свързани със злоупотреба с устройства и мрежи:

- Приложения, които блокират друго показващо реклами приложение или възпрепятстват работата му.
- Приложения за улесняващи играта хитрини, които влияят на начина на игра в други приложения.
- Приложения, които улесняват или предоставят инструкции за извършването на непозволен промени в услуги, софтуер или хардуер или заобикалят защитните механизми.
- Приложения, които използват или осъществяват достъп до услуга или API по начин, нарушаващ съответните общи условия;
- Приложения, които не [отговарят на условията за поставяне в списъка с разрешени](#) и опитват да заобиколят [системните функции за управление на консумацията](#).
- Приложения, които улесняват прокси услуги към трети страни, се допускат само ако това е основната им функция, насочена към потребителя.
- Приложения или код на трети страни (например SDK), които изтеглят изпълним код, например dex файлове или код с директно изпълнение, от източник, различен от Google Play.
- Приложения, които инсталират други приложения на устройството без предварителното съгласие на потребителя;
- Приложения, които водят към злонамерен софтуер или улесняват разпространението или инсталирането на такъв.
- Приложения или код на трети страни (например SDK), които съдържат WebView с добавен интерфейс на JavaScript, който зарежда ненадеждно уеб съдържание (например URL адрес с http://) или непотвърдени URL адреси, получени от ненадеждни източници (например URL адреси, получени от ненадеждни намерения).
- Приложения, които използват [разрешение за намерение за цял екран](#) с цел принуждаване на потребителя да взаимодейства с натрапчиви реклами или известия.

Използване на услуги на преден план

Разрешението за услуга на преден план осигурява уместното използване на услуги на преден план, взаимодействащи с потребителя. Когато приложенията са насочени към Android 14 или по-нова версия, за всяка използвана в тях услуга на преден план трябва да посочите валиден тип и да декларирате подходящото за този тип [разрешение за такава услуга](#). Ако например за използването на приложението ви е необходима геолокация на картата, в манифеста му трябва да декларирате разрешението `FOREGROUND_SERVICE_LOCATION`.

На приложенията е разрешено да декларират разрешение за услуга на преден план само в случай че използването ѝ:

- осигурява функция, която е полезна за потребителя и е свързана с основната функционалност на приложението;
- се стартира от потребителя или може да бъде разпознато от него (например звук при възпроизвеждане на песен, предаване на мултимедийно съдържание към друго устройство, точно и ясно известие за потребителя, заявка от потребителя за качване на снимка в облака);
- може да бъде прекратено или спряно от потребителя;
- не може да бъде прекъснато или отложено от системата, без това да причини отрицателна практическа работа на потребителя или да доведе до това, очакваната от потребителя функция да не работи според очакванията (например телефонно обаждане трябва да започне незабавно и не може да бъде отложено от системата);
- трае само през времето, необходимо за изпълнение на задачата.

Изключения от горепосочените критерии са следните случаи на използване на услуги на преден план:

- типовете услуги на преден план `systemExempted` или `shortService`;
- типовете услуги на преден план `dataSync` само когато се използват функциите на [Play Asset Delivery](#).

Използването на услугите на преден план е обяснено по-подробно [тук](#).

Започнати от потребителя задания за прехвърляне на данни

На приложенията е разрешено да използват API за [започнати от потребителя задания за прехвърляне на данни](#) само ако съответното използване:

- е започнато от потребителя;
- служи за задачи по прехвърляне на данни в мрежата;
- трае само през времето, необходимо за прехвърлянето на данните.

Използването на API за започнати от потребителя задания за прехвърляне на данни е обяснено по-подробно [тук](#).

Изисквания за Flag Secure

`FLAG_SECURE` е флаг за показване, деклариран в кода на дадено приложение. Той указва, че ПИ съдържа чувствителни данни, които трябва да бъдат ограничени до сигурни места, докато приложението се използва. Флагът е създаден с цел да се предотврати показването на данните в екранни снимки или преглеждането им по несигурен начин. Програμισите декларират този флаг, когато съдържанието на приложението не трябва се предава, преглежда или прехвърля по друг начин извън приложението или устройството на потребителя.

От съображения за сигурност и поверителност всички разпространявани в Google Play приложения трябва да зачитат декларирането на `FLAG_SECURE` от други приложения. Това означава, че приложенията не трябва да улесняват или да създават начини за заобикаляне на настройките `FLAG_SECURE` в други приложения.

Приложенията, които се квалифицират като [инструмент за достъпност](#) , са освободени от това изискване, при условие че не предават, запазват или кешират защитено чрез FLAG_SECURE съдържание за достъп извън устройството на потребителя.

Приложения, които стартират локалните контейнери на Android

Приложенията с локални контейнери за Android предоставят среди, които имитират цялата операционна система Android или части от нея. Практическата работа в тези среди може да не отразява пълния пакет [функции за сигурност на Android](#) . Поради това програмистите могат да добавят флаг за сигурна среда в манифеста, който да посочва на локалните контейнери за Android, че не трябва да работят в среда, имитираща операционната система.

Флаг за манифест за сигурна среда

`REQUIRE_SECURE_ENV` представлява флаг, който може да бъде деклариран в манифеста на дадено приложение, за да се посочи, че то не трябва да се изпълнява в локални контейнери за Android. От съображения за сигурност и поверителност приложенията, които предоставят локални контейнери за Android, трябва да зачитат всички приложения, декларирали този флаг, и:

- да потърсят този флаг в манифестите на приложенията, които възнамеряват да заредят в локалните си контейнери за Android;
- да не зареждат приложенията, които са декларирали този флаг, в локалните си контейнери за Android;
- да не функционират като прокси сървър, който прехваща или извиква API на устройството, така че да изглежда, че са инсталирани в контейнера;
- да не улесняват, нито да създават начини за заобикалянето на флага (като например зареждане на по-стара версия на дадено приложение с цел да се заобиколи флага `REQUIRE_SECURE_ENV` на текущото приложение).

Научете повече за тези правила в нашия [Помощен център](#).

Подвеждащо поведение

Не разрешаваме приложения, които опитват да подвеждат потребителите или допускат непочтено поведение, включително, но не само, приложения, чиято функционалност е определена за невъзможна. Приложенията трябва да представят точно функционалността си чрез разкриване на информация, описание и изображения/видеоклипове във всички части от метаданните. Те не трябва да имитират функции или предупреждения от операционната система или от други приложения. Всички промени в настройките на устройството трябва да се извършват със знанието и съгласието на потребителя и да са обратими.

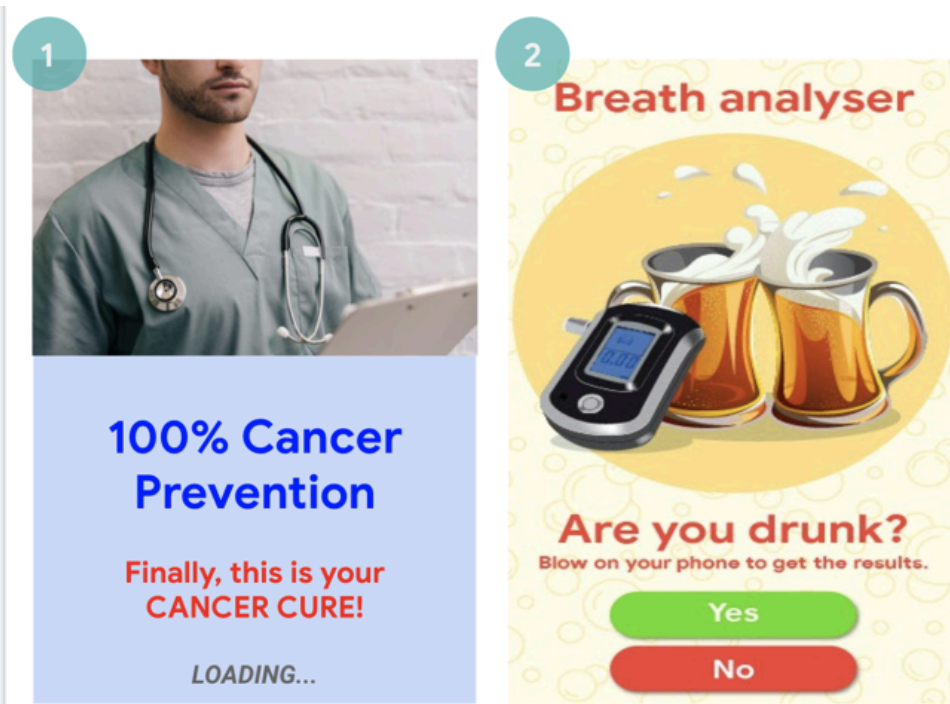
Подвеждащи изявления

Не допускаме приложения, които съдържат невярна или подвеждаща информация или твърдения, включително в описанието, името, иконата и екранните снимки.

Ето няколко примера за често срещани нарушения:

- Приложения, чиято функционалност не е описана точно и ясно или сведенията за нея са по същество погрешни:
 - Приложение, в чието описание и екранни снимки се твърди, че е състезателна игра, но всъщност е пъзел с кубчета, за който се използва изображение на автомобил.
 - Приложение, за което се твърди, че е антивирусна програма, но съдържа само текстово ръководство, обясняващо как да премахвате вируси.

- Приложения, за които се твърди, че имат невъзможни за реализиране функции (като например приложения за отблъскване на насекоми), дори ако са представени като шега, номер, измислица и гр.
- Приложения, които са неправилно категоризирани, включително, но не само, чрез класификацията или категорията на приложението.
- Явно измамно или фалшиво съдържание, което може да попречи на изборните процеси или на резултата от тях.
- Приложения, за които невярно се твърди, че са свързани с правителствена организация, или които предоставят или изпълняват правителствени услуги, за които не са надлежно упълномощени.
- Приложения, за които невярно се твърди, че са официалното приложение на определен субект. Имена като Justin Bieber Official не са позволени без необходимите разрешения или права.



- (1) В това приложение има медицински или свързани със здравето твърдения (лекува рак), които са подвеждащи.
- (2) За това приложение се твърди, че има невъзможни за реализиране функции (използва телефона ви като грезер).

Подвеждащи промени в настройките на устройството

Не допускаме приложения, които извършват промени в настройки или функции на устройството извън рамките си без знанието и съгласието на потребителя. Това включва настройките на системата и браузъра, отметките, преките пътища, иконите, приспособленията, както и представянето на приложенията на началния екран.

Освен това не позволяваме:

- Приложения, които променят настройки или функции на устройството със съгласието на потребителя, но по начин, който не е лесно обратим.
- Приложения или реклами, които променят настройки или функции на устройството като услуга към трети страни или за рекламни цели.
- Приложения, които подвеждат потребителите да премахват или деактивират приложения на трети страни или да променят настройки или функции на устройството.

- Приложения, които насърчават или подтикват потребителите да премахват или деактивират приложения на трети страни или да променят настройки или функции на устройството, освен ако това не е част от услуга за сигурност, която може да бъде проверена.

Допускане на непочтено поведение

Не допускаме приложения, които помагат на потребителите да подвеждат други хора или по някакъв начин са измамни по отношение на функционалността си, включително, без избораването да е изчерпателно, такива за генериране или улесняване на генерирането на документи за самоличност, единни граждански номера, паспорти, дипломи, кредитни карти, банкови сметки и шофьорски книжки. Приложенията трябва да представят точно функционалността и/или съдържанието си чрез разкриване на информация, заглавия, описания и изображения/видеоклипове и да работят според основателните очаквания на потребителя.

Изтеглянето на допълнителни ресурси за приложението (например активи в игра) е разрешено само ако са необходими за използването му от потребителите. Изтегляните ресурси трябва да спазват всички правила на Google Play и преди изтеглянето да започне, в приложението трябва да се показва подкана за потребителите и ясно да е посочен размерът на съответния файл.

Твърденията, че дадено приложение е „шега“ или „с развлекателна цел“ (или други синоними), не го освобождават от прилагането на правилата ни.

Ето няколко примера за често срещани нарушения:

- Приложения, които имитират други приложения или уебсайтове, за да подведат потребителите да разкрият лични или удостоверителни данни;
- Приложения, които изобразяват или показват непотвърдени или истински телефонни номера, информация за връзка, адреси или информация, позволяваща лично идентифициране, на физически или юридически лица без тяхно съгласие;
- Приложения с различна основна функционалност въз основа на географското местоположение, параметрите на устройството или други данни, които зависят от потребителя, когато тези разлики не са ясно посочени в малката обява в магазина;
- Приложения, при които има значителна промяна от предходната версия, без потребителят да бъде уведомен (напр. в [секцията „Новите неща“](#)) и да се актуализира малката обява в магазина;
- Приложения, които се опитват да променят или прикрият поведението си по време на преглед;
- Приложения, които изтеглят файлове през мрежа за доставяне на съдържание (CDN), без преди това да покажат подкана на потребителите и да им предоставят информация за размера на съответните файлове.

Манипулирана масова информация

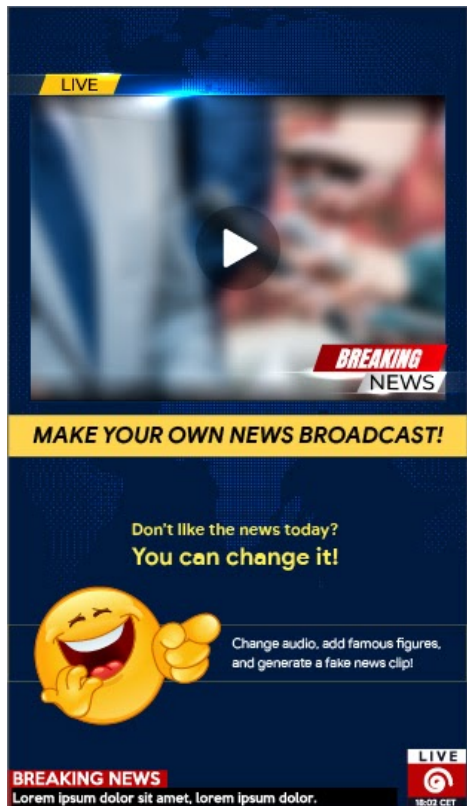
Не допускаме приложения, които насърчават или подпомагат създаването на неверни или подвеждащи твърдения или информация, предавани чрез изображения, аудио, видеоклипове и/или текст. Забраняваме приложенията, предназначени да популяризират или разпространяват видимо подвеждащи или измамни изображения, видеоклипове и/или текст, които може да причинят вреда във връзка с деликатно събитие, политическа тема, социални проблеми или други въпроси от обществено значение.

Приложенията, които манипулират или променят масова информация отвъд конвенционалните и редакционно приемливи корекции за яснота и качество, трябва ясно да разкриват или обозначават промените, когато те не са лесно разграничими за обикновения

потребител. Възможно е да направим изключение, ако промяната е в обществен интерес или има сатиричен или пародиен характер.

Ето няколко примера за често срещани нарушения:

- Приложения, които създават впечатление, че обществена личност е присъствала на демонстрация по време на деликатно политическо събитие.
- Приложения, които използват обществени личности или мултимедийно съдържание от деликатно събитие, за да популяризират възможността си за промяна на масова информация в малката си обява в магазина;
- Приложения, които променят клипове от медиите, за да имитират новинарска емисия.



(1) Това приложение осигурява функционалност за промяна на клипове от медиите, за да се имитира новинарска емисия, и добавяне на известни или обществени личности към клипа без воден знак.

Прозрачност на поведението

Функционалността на приложението ви трябва да бъде сравнително ясна за потребителите. Не включвайте скрити, неактивни или недокументирани функции в него. Не се допускат техники за избягване на отзивите за приложението. Може да се наложи да бъдат предоставени допълнителни подробности за приложенията с цел да се гарантират безопасността на потребителите, целостта на системата и спазването на правилата.

Подвеждащо представяне

Не допускаме приложения или профили на програмисти, които:

- се представят за други лица или организации, както и такива, които представят невярно или прикриват собственика или основната си функция.
- участват в координирана дейност за подвеждане на потребители. Това включва, но не се ограничава до приложения или профили, които представят невярно или прикриват

държащата си на произход или които насочват съдържание към потребители в друга държава.

- се координират с други приложения, сайтове, програмисти или профили, за да прикрият или да представят по подвеждащ начин самоличността на програмиста/идентифицираща приложението информация или други съществени подробности, когато съдържанието на приложението е свързано с политика, социални въпроси или такива от обществено значение.

Правила на Google Play за целевото ниво на API

Google Play ще изисква от **всички приложения** да използват целевите нива на API по-долу с цел осигуряване на безопасна и сигурна практическа работа на потребителите:

Новите приложения и актуализации на приложения ТРЯБВА да са с целево ниво на API, пуснато до една година преди най-новата пусната основна версия на Android. Изпращането в Play Console на нови приложения и актуализации, които не отговарят на това изискване, няма да бъде възможно.

Съществуващите приложения в Google Play, които не са актуализирани и не са с целево ниво на API, пуснато до две години преди най-новата основна версия на Android, няма да са налице за нови потребители, чиито устройства са с по-нова версия на операционната система. Потребителите, които по-рано са инсталирали приложението от Google Play, ще запазят възможността си да го откриват, преинсталират и използват на поддържаните от него версии на Android.

За технически съвети относно това, как да спазите изискването за целевото ниво на API, вижте [ръководството относно мигрирането](#).

За конкретни срокове и изключения направете справка с тази статия в [Помощния ни център](#).

Изисквания за SDK

Програмистите на приложения често разчитат на код на трети страни (например SDK), за да интегрират ключови функционалности и услуги в приложенията си. Когато включвате SDK в приложението си, трябва да се уверите, че потребителите ви са в безопасност и че приложението ви е защитено от уязвимости. В тази секция демонстрираме как част от съществуващите ни изисквания за поверителност и сигурност се прилагат в контекста на SDK. Те имат за цел да помогнат на програмистите да интегрират SDK в приложенията си по безопасен и сигурен начин.

Ако включите SDK в приложението си, трябва да се уверите, че то не нарушава програмните правила за програмистите в Google Play поради кода и практиките на съответната трета страна. Важно е да обърнете внимание на начина, по който използваните в приложението ви SDK боравят с потребителските данни, и да знаете какви разрешения използват, какви данни събират и защо. Не забравяйте, че събирането и обработването на потребителски данни от страна на гаген SDK трябва да съответства на спазващия правилата начин, по който приложението ви използва съответните данни.

За да се уверите, че използван от вас SDK не нарушава изискванията на правилата, прочетете внимателно и изцяло посочените по-долу правила и обърнете внимание на следните им съществуващи изисквания, свързани с SDK:

Правила за потребителските данни

Трябва да има прозрачност в начина, по който боравите с потребителските данни (например информация, събрана от или за потребителя, включително за устройството). Това означава да разкривате достъпа, събирането, използването, обработването и

споделянето на потребителски данни от страна на приложението ви и да ги използвате само за оповестените цели, които спазват правилата.

Ако сте включили код на трета страна (например SDK) в приложението си, трябва да се уверите, че съответният код, както и практиките на третата страна по отношение на потребителските данни от приложението ви спазват програмните правила за програмистите в Google Play, които включват изисквания за употреба и разкриване на информация. Трябва например да се уверите, че доставчиците ви на SDK не продават лични и чувствителни потребителски данни от приложението ви. Това изискване е в сила независимо дали потребителските данни се предават след изпращане до сървър, или чрез въграждане на код на трета страна в приложението ви.

Лични и чувствителни потребителски данни

- Ограничете достъпа, събирането, използването и споделянето на лични и чувствителни потребителски данни, получени чрез приложението, като извършвате тези действия само за функции на приложения и услуги, както и за съобразени с правилата цели според основателните очаквания на потребителя:
 - Приложенията, които разширяват употребата на личните и чувствителните данни до показване на реклами, трябва да спазват правилата на Google Play за рекламите.
- Трябва да боравите с всички лични и чувствителни потребителски данни по сигурен начин, включително да ги предавате посредством съвременни криптографски решения (например през HTTPS).
- При възможност използвайте заявка за разрешения по време на изпълнение, преди да осъществите достъп до данни, ограничени от разрешения за Android.

Продажба на лични и чувствителни потребителски данни

Не продавайте личните и чувствителните потребителски данни.

- „Продажба“ е обменът или предаването на лични и чувствителни потребителски данни към трети страни срещу финансова облага.
- Започнато от потребителя предаване на лични и чувствителни потребителски данни (когато например потребителят използва функция на приложението, за да прехвърли файл към трета страна, или когато той по собствено желание използва специално приложение за научно изследване) не се смята за продажба.

Изисквания за разкриване на информация по ясен начин и получаване на съгласие

В случаите, когато достъпът, събирането, използването и споделянето на лични и чувствителни потребителски данни може да са извън основателните очаквания на потребителя за въпросния продукт или функция, трябва да изпълните изискванията, посочени в [правилата за потребителските данни](#), за разкриване на информация по ясен начин и получаване на съгласие.

Ако в приложението ви е интегриран код на трета страна (например SDK), чието стандартно предназначение е да събира лични и чувствителни потребителски данни, в рамките на 2 седмици от получаването на искане от Google Play (или в рамките на по-дълъг период от време, ако е посочен такъв в искането от Google Play) трябва да предоставите достатъчно доказателства в подкрепа на това, че приложението ви спазва изложените в текущите правила изисквания за разкриване на информация по ясен начин и получаване на съгласие, включително по отношение на достъпа, събирането, използването и споделянето на данни посредством кода на трета страна.

Не забравяйте да се уверите, че с използването на код на трета страна (например SDK) приложението ви не нарушава [правилата за потребителските данни](#).

За повече информация относно изискването за разкриване на информация по ясен начин и получаване на съгласие вижте тази статия в [Помощния център](#).

Примери за нарушения, причинени от SDK

- Приложение с SDK, който събира лични и чувствителни потребителски данни и не ги третира като предмет на текущите правила за потребителските данни и на изискванията, свързани с достъпа и обработването на данните (включително непозволената продажба), и тези за разкриване на информация по ясен начин и получаване на съгласие.

- Приложение, в което е интегриран SDK, събира лични и чувствителни потребителски данни по подразбиране, като по този начин нарушава изискванията на настоящите правила относно получаване на съгласие от потребителя и разкриване на информация по ясен начин.
- Приложение с SDK, за който се твърди, че събира лични и чувствителни потребителски данни само с цел обезпечаване на функции, предотвратяващи измами и злоупотреба, но съответният SDK също споделя с трети страни събираните от него данни с цел рекламиране или анализ.
- Приложение, включващо SDK, който предава информация за инсталираните от потребителя пакети, без да спазва указанията за разкриване на информация по ясен начин и/или [указанията за декларация за поверителност](#).
- Вижте и правилата относно [нежелания софтуер на мобилни устройства](#).

Допълнителни изисквания за достъп до личните и чувствителните данни

В таблицата по-долу са описани изискванията за конкретни активности.

Активност	Изискване
Приложението ви събира постоянни идентификатори на устройството или прави връзки с тях (напр. IMEI, IMSI, серийния номер на SIM картата и др.)	Постоянните идентификатори на устройството не бива да се свързват с други лични и чувствителни потребителски данни или идентификатори на устройства, които могат да бъдат нулирани, освен за следните цели: • телефонни услуги, свързани с конкретна SIM карта (напр. обаждания през Wi-Fi, свързани с профил към оператор); • приложения за управление на корпоративно устройство, които използват режима за собственик на устройството. Тези начини на използване трябва да бъдат представени на потребителите по ясен начин, както е описано в правилата за потребителските данни. За алтернативните уникални идентификатори прегледайте този ресурс. За допълнителни указания относно идентификатора за рекламиране за Android прочетете правилата за рекламите.
Приложението ви е насочено към деца	Приложението ви може да включва само SDK, които са самостоятелно сертифицирани за употреба в насочени към деца услуги. За пълните правила и изисквания прегледайте страницата Програма за самостоятелно сертифицирани SDK за реклами за семейства.

Примери за нарушения, причинени от SDK

- Приложение, използващо SDK, който свързва идентификатор за Android с местоположението.
- Приложение с SDK, който свързва AAID с постоянните идентификатори на устройството с цел рекламиране или анализ.
- Приложение, използващо SDK, който свързва AAID с имейл адрес с цел анализ.

Секция за безопасност на данните

Всички програмисти трябва да попълнят ясно и точно секцията за безопасност на данните за всяко приложение, като предоставят информация относно събирането, използването и споделянето на потребителски данни. Това включва данните, събирани и обработвани чрез използваните в приложенията им библиотеки или SDK на трети страни. Програмистите носят отговорност за точността на етикета за поверителността и актуализирането на тези данни. Където е уместно, информацията в секцията трябва да съответства на разкриванията в декларацията за поверителност на приложението.

Направете справка с тази статия в [Помощния център](#) за допълнителна информация относно попълването на секцията за безопасност на данните.

Вижте пълния текст на [правилата за потребителските данни](#).

Правила относно разрешенията и API, които осъществяват достъп до поверителна информация

Исканията за разрешения и използване на API, които осъществяват достъп до поверителна информация, трябва да са разбираеми за потребителите. Може да искате само разрешения и да ползвате API с достъп до поверителна информация, когато това е необходимо за реализирането на текущи функции или услуги в приложението Ви, посочени в малката обява за него в Google Play. Не може да използвате разрешения и API с достъп до поверителна информация, които дават достъп до потребителски данни или такива за устройството, за неразкрити, нереализирани или забранени функции или цели. Забранено е лични или чувствителни данни, получени чрез тези разрешения или API, да се продават или споделят с цел улесняване на продажбата им.

Вижте пълния текст на [правилата относно разрешенията и API, които осъществяват достъп до поверителна информация](#).

Примери за нарушения, причинени от SDK

- Приложението Ви включва SDK, който иска достъп до местоположението на заден план за забранена или неразкрита цел.
- Приложението Ви включва SDK, който предава IMEI, извлечен посредством разрешението за Android read_phone_state, без съгласието на потребителя.

Правила относно злонамерения софтуер

Правилата ни относно злонамерения софтуер са прости – екосистемата на Android, включително Google Play Магазин, и устройствата на потребителите не трябва да бъдат обект на опасно (т.е. злонамерено) поведение. Това е основният принцип, въз основа на който се стремим да осигуряваме екосистема на Android, която е безопасна за потребителите и устройствата им.

Злонамерен софтуер е всеки код, който може да застраши даден потребител, данните или устройството му. Злонамереният софтуер включва, без изброяването да е изчерпателно, потенциално опасни приложения, гвочен код или промени в софтуерната рамка и се състои от различни категории, като например троянски коне, приложения за фишинг и шпионирещ софтуер. Непрекъснато актуализираме списъка с категории и добавяме нови.

Изискванията на тези правила се отнасят и за кодовете на трети страни (например SDK), които включвате в приложението си.

Вижте пълния текст на [правилата относно злонамерения софтуер](#).

Примери за нарушения, причинени от SDK

- Приложения, включващи библиотеки с SDK от доставчици, които разпространяват злонамерен софтуер.
- Приложения, които нарушават модела за разрешения на Android или крадат идентификационни данни (например означения за OAuth) от други приложения.
- Приложения, които злоупотребяват с функции, за да предотвратят деинсталирането или спирането си.
- Приложения, които деактивират SELinux.
- Приложения, които включват SDK, който не спазва модела за разрешения на Android, като получава администраторски права чрез достъп до данните на устройството за неразкрита цел.
- Приложения, които включват SDK с код, който подвежда потребителите да се абонират или да купят съдържание чрез сметката за мобилния си телефон.

Използване на SDK в приложения

Ако включите SDK в приложението си, трябва да се уверите, че то не нарушава програмните правила за програмистите в Google Play поради кода и практиките на съответната трета страна. Важно е да обърнете внимание на начина, по който използваните в приложението ви SDK боравят с потребителските данни, и да знаете какви разрешения използват, какви данни събират и защо.

Изисквания за SDK

Програмистите на приложения често разчитат на код на трети страни (например SDK), за да интегрират ключови функционалности и услуги в приложенията си. Когато включвате SDK в приложението си, трябва да се уверите, че потребителите ви са в безопасност и че приложението ви е защитено от уязвимости. В тази секция демонстрираме как част от съществуващите ни изисквания за поверителност и сигурност се прилагат в контекста на SDK. Те имат за цел да помогнат на програмистите да интегрират SDK в приложенията си по безопасен и сигурен начин.

Ако включите SDK в приложението си, трябва да се уверите, че то не нарушава програмните правила за програмистите в Google Play поради кода и практиките на съответната трета страна. Важно е да обърнете внимание на начина, по който използваните в приложението ви SDK боравят с потребителските данни, и да знаете какви разрешения използват, какви данни събират и защо. Не забравяйте, че събирането и обработването на потребителски данни от страна на даден SDK трябва да съответства на спазващия правилата начин, по който приложението ви използва съответните данни.

За да се уверите, че използван от вас SDK не нарушава изискванията на правилата, прочетете внимателно и изцяло посочените по-долу правила и обърнете внимание на следните им съществуващи изисквания, свързани с SDK:

Приложения, които си осигуряват администраторски права и получават пълноправен достъп до устройствата без разрешението на потребителите, се класифицират като приложения за пълноправен достъп.

Шпиониращ софтуер

Шпиониращият софтуер е злонамерено приложение, код или действие за събиране, извличане или споделяне на потребителски данни или данни от устройството за цели, които не са свързани със спазващата правилата функционалност.

Злонамереният код и действията, които могат да бъдат сметнати за шпиониране на потребителя или при които се извличат данни без съответното известие или получаване на съгласие, също може да попаднат в категорията за шпиониращ софтуер.

Вижте пълния текст на [правилата относно шпиониращия софтуер](#).

Примерите за причинени от SDK нарушения на правилата относно шпиониращия софтуер включват, но не се ограничават до:

- приложение, използващо SDK, който предава данни от аудиозаписи или записи на обаждания, когато това не е свързано със спазваща правилата функционалност на приложението;
- приложение със злонамерен код на трета страна (например SDK), който предава данни извън устройството по неочакван за потребителя начин и/или без съответното известие или без съгласието на потребителя.

Правила относно нежелания софтуер на мобилни устройства

Прозрачно поведение и разкриване по ясен начин

Всеки код трябва да изпълнява дадените на потребителя обещания. Приложенията трябва да осигуряват всички обявени функционалности. Приложенията не трябва да объркват потребителите.

Примери за нарушения:

- измама с реклами;
- социално инженерство.

Защитавайте потребителските данни

Осигурете яснота и прозрачност по отношение на достъпа, използването, събирането и споделянето на лични и чувствителни потребителски данни. При използване на потребителски данни трябва да се спазват съответните правила, където е приложимо, и да се вземат всички предпазни мерки за защита на данните.

Примери за нарушения:

- събиране на данни (направете справка с раздела „Шпиониращ софтуер“);
- злоупотреба с ограничени разрешения.

Вижте пълния текст на [правилата относно нежелания софтуер на мобилни устройства](#)

Правила относно злоупотребата с устройства и мрежи

Не допускаме приложения, които могат да повредят, да възпрепятстват или влошат работата на или да осъществяват неупълномощен достъп до устройството на потребителя, други устройства или компютри, сървъри, мрежи, приложни програмни интерфейси (API) или услуги, включително, но не само, други приложения на устройството, която и да е услуга на Google или мрежата на оторизиран оператор.

Приложения или код на трета страна (напр. SDK), съдържащи интерпретируеми езици (JavaScript, Python, Lua и др.), които се зареждат по време на изпълнение (напр. такива, които не са пакетирани с приложението), не трябва да допускат потенциални нарушения на правилата на Google Play.

Не допускаме код, който въвежда или използва уязвимости в сигурността. Разгледайте [програмата за подобряване на сигурността на приложенията](#), за да научите повече за най-скорошните проблеми със сигурността, за които е подаден сигнал до програмистите.

Вижте пълния текст на [правилата относно злоупотребата с устройства и мрежи](#).

Примери за нарушения, причинени от SDK

- Приложения, които улесняват прокси услуги към трети страни, се допускат само ако това е основната им функция, насочена към потребителя.
- Приложението ви включва SDK, който изтегля изпълним код, като например dex файлове или код с директно изпълнение, от източник, различен от Google Play.
- Приложението ви включва SDK, съдържащ WebView с добавен интерфейс на JavaScript, който зарежда ненадежно уеб съдържание (например HTTP URL адрес) или непотвърдени URL адреси, получени от ненадежни източници (например URL адреси, получени от ненадежни намерения).
- Приложението ви включва SDK, съдържащ код, който се използва за актуализиране на собствения му APK файл.
- Приложението ви включва SDK, който излага потребителите на уязвимост в сигурността, като изтегля файлове през незащитени връзки.
- Приложението ви включва SDK, който съдържа код за изтегляне и инсталиране на приложения от неизвестни източници извън Google Play.

- Приложението ви включва SDK, който използва услуги на преден план без подходящ случай на употреба.
- Приложението ви включва SDK, който използва услуги на преден план съгласно правилата, но случаят на употреба не е деклариран в манифеста на приложението ви.

Правила относно подвеждащото поведение

Не разрешаваме приложения, които опитват да подвеждат потребителите или допускат непочтено поведение, включително, но не само, приложения, чиято функционалност е определена за невъзможна. Приложенията трябва да представят точно функционалността си чрез разкриване на информация, описание и изображения/видеоклипове във всички части от метаданните. Те не трябва да имитират функции или предупреждения от операционната система или от други приложения. Всички промени в настройките на устройството трябва да се извършват със знанието и съгласието на потребителя и да са обратими.

Вижте пълния текст на [правилата относно подвеждащото поведение](#).

Прозрачност на поведението

Функционалността на приложението ви трябва да бъде сравнително ясна за потребителите. Не включвайте скрити, неактивни или недокументирани функции в него. Не се допускат техники за избягване на отзивите за приложението. Може да се наложи да бъдат предоставени допълнителни подробности за приложенията с цел да се гарантират безопасността на потребителите, целостта на системата и спазването на правилата.

Пример на причинено нарушение от SDK

- Приложението ви включва SDK, който използва техники за избягване на отзивите за приложението.

Кои правила за програмистите в Google Play обикновено се свързват с нарушенията, причинени от SDK?

За да се уверите, че използваният в приложението ви код на трета страна спазва програмните правила за програмистите в Google Play, вижте пълния текст на посочените по-долу правила:

- [Правила за потребителските данни](#)
- [Разрешения и API, които осъществяват достъп до поверителна информация](#)
- [Правила относно злоупотребата с устройства и мрежи](#)
- [Злонамерен софтуер](#)
- [Нежелан софтуер на мобилни устройства](#)
- [Програма за самостоятелно сертифицирани SDK за реклами за семейства](#)
- [Правила за рекламите](#)
- [Подвеждащо поведение](#)
- [Програмни правила за програмистите в Google Play](#)

Въпреки че обикновено възникват проблеми с тези правила, важно е да не забравяте, че поради проблемен код на SDK приложението ви може да наруши правило, което не е споменато по-горе. Не забравяйте да прегледате пълния текст на всички правила, за да получите актуална информация. Като програмист трябва да се уверите, че използваните от вас SDK боравят с данните от приложението ви по спазващ правилата начин.

За да научите повече, посетете [Помощния ни център](#).

Злонамерен софтуер

Правилата ни относно злонамерения софтуер са прости – екосистемата на Android, включително Google Play Магазин, и устройствата на потребителите не трябва да бъдат обект на опасно (т.е. злонамерено) поведение. Това е основният принцип, въз основа на който се стремим да осигуряваме екосистема на Android, която е безопасна за потребителите и устройствата им.

Злонамерен софтуер е всеки код, който може да застраши даден потребител, данните или устройството му. Злонамереният софтуер включва, без изброяването да е изчерпателно, потенциално опасни приложения, двоичен код или промени в софтуерната рамка и се състои от различни категории, като например троянски коне, приложения за фишинг и шпиониращ софтуер. Непрекъснато актуализираме списъка с категории и добавяме нови.

Изискванията на тези правила се отнасят и за коговете на трети страни (например SDK), които включвате в приложението си.

Въпреки че се различава по тип и възможности, злонамереният софтуер обикновено има една от следните цели:

- Компрометиране на целостта на устройството на потребителя.
- Установяване на контрол над устройството на потребителя.
- Даване на възможност за извършване на отдалечени действия, чрез които хакер да получи достъп до заражено устройство, да го използва или да се възползва от него по друг начин.
- Предаване на лични или идентификационни данни извън устройството без съответното съобщение за разкриване и без получаване на съгласие.
- Разпространяване на спам или команди от заразеното устройство с цел да се повлияе на други устройства или мрежи.
- Подвеждане на потребителя.

Дадено приложение, двоичен код или промяна в софтуерната рамка могат да бъдат потенциално опасни и така да създадат предпоставка за злонамерено поведение, дори да не са били предназначени за това. Причината е, че приложенията, двоичният код и промените в софтуерната рамка могат да функционират различно в зависимост от редица променливи. Това означава, че нещо, което е опасно за едно устройство с Android, може да не представлява никакъв риск за друго. Например устройство с най-новата версия на Android не е засегнато от опасни приложения, които използват оттеглени API за злонамерени цели, но такова с много стара версия на Android може да е застрашено. Приложения, двоичен код или промени в софтуерната рамка се означават като злонамерен софтуер или като потенциално опасни, ако е ясно, че представляват риск за някои или всички устройства с Android и потребители на операционната система.

Категориите злонамерен софтуер по-году са отражение на фундаменталния ни принцип, че потребителите трябва да разбират как се използва устройството им, и на стремежа ни за създаване на сигурна екосистема, която дава възможност за устойчиви нововъведения и надеждна практическа работа на потребителите.

За повече информация посетете [Google Play Protect](#) .

Задни врати

Код, който позволява изпълнението на нежелани, потенциално опасни и отдалечено контролирани операции на дадено устройство.

Тези операции може да включват поведение, при чиято автоматична проява приложението, двоичният код или промяната в софтуерната рамка може да попаднат в една от другите категории злонамерен софтуер. По принцип „задната врата“ представлява описание на това, как потенциално опасно действие може да бъде извършено на устройство, и поради тази причина не попада изцяло в категории като измама с таксуване или комерсиален

шпиониращ софтуер. В резултат на това при определени обстоятелства Google Play Protect третира някои „задни врати“ като уязвимост.

Измама с таксуване

Код, чрез който потребителят автоматично се таксува по целенасочено подвеждащ начин.

Измата с мобилно таксуване се дели на няколко вида – с SMS, с обаждания и с начисляване на такса.

Измама с SMS

Код, при който без съгласието на потребителите те се таксуват за изпращането на SMS с допълнителна такса, или код, който се опитва да прикрие действията си с SMS, като крие споразуменията за разкриване на информация или SMS съобщенията от мобилния оператор, уведомяващи потребителя за таксите или потвърждаващи абонаментите.

Някои видове код, макар технически да разкриват изпращането на SMS, имат и друго поведение, с което се извършват измами с SMS. Примерите включват скриването от потребителя на части от споразумението за разкриване на информация, като се правят нечетими, и спирането при определени условия на SMS съобщенията от мобилния оператор, уведомяващи потребителя за таксите или потвърждаващи абонаментите.

Измама с обаждания

Код, при който потребителите се таксуват, като без тяхно съгласие се извършват обаждания до номера с допълнително таксуване.

Измама с начисляване на такса

Код, който подвежда потребителите да се абонират или да купят съдържание чрез сметката за мобилния си телефон.

Измата с начисляване на такса включват всички типове таксуване без тези от SMS съобщенията и обажданията с допълнителни такси. Примерите включват директно таксуване от оператор, безжична точка за достъп (WAP) и прехвърляне на кредити за мобилната мрежа. Измата с WAP е една от най-често срещаните измами с начисляване на такса. Тя може да включва подвеждане на потребителите да кликнат върху бутон в негласно зареден прозрачен компонент WebView. При извършването на това действие се стартира подновяващ се абонамент и често SMS съобщението или имейлът за потвърждение се прехващат, така че потребителите да не забележат финансовата транзакция.

Шпионски софтуер

Код, който събира лични или поверителни потребителски данни от дадено устройство и ги предава на трета страна (организация или физическо лице) с цел наблюдение.

Приложенията трябва да разкриват съответната информация по ясен начин и да получат съгласие, както се изисква в [правилата за потребителските данни](#).

Указания за приложенията за наблюдение

Единствените приемливи приложения за наблюдение са тези, които са изрично проектирани и се предлагат за наблюдение на други лица (например за родители, за да наблюдават децата си, или за корпоративно управление с цел наблюдението на отделни служители), при условие че напълно отговарят на описаните по-долу изисквания. Тези приложения не могат да се използват за слеждане на други хора (например съпруг или съпруга) дори ако човекът е уведомен и е дал разрешение за това, независимо дали се показва постоянно известие. Тези приложения трябва да използват във файла на манифеста си флага за метаданни IsMonitoringTool, за да бъдат представяни правилно като приложения за наблюдение.

Приложенията за наблюдение трябва да спазват следните изисквания:

- Не трябва да се представят като решения за шпиониране или тайно наблюдение.

- Не трябва да скриват или прикриват проследяващото поведение, нито да опитват да подвеждат потребителите относно подобна функционалност.
- Трябва да показват постоянно известие винаги когато се изпълняват, както и уникална икона, която ясно да идентифицира съответното приложение.
- Функционалността на приложенията за наблюдение или проследяване трябва да е ясно посочена в описанието в Google Play Магазин.
- Приложенията и малките им обяви в Google Play не трябва да осигуряват средства за активиране на или достъп до функционалност, която нарушава тези условия, като например връзки към неспазващ правилата APK файл, хостван извън Google Play.
- Приложенията трябва да спазват всички приложими закони. Вие носите цялата отговорност за определяне на законността на приложението си в целевите локали.

За повече информация, моля, разгледайте статията [Използване на флага IsMonitoringTool](#) в Помощния център.

Отказ от обслужване (DoS)

Код, който без знанието на потребителя извършва атака за отказ от обслужване (DoS) или е част от разпределена DoS атака срещу други системи и ресурси.

Например това може да се случи чрез изпращането на голям брой HTTP заявки с цел създаване на прекомерно натоварване на отдалечени сървъри.

Злонамерени инструменти за изтегляне

Код, който сам по себе си не е потенциално опасен, но изтегля групи PHA.

Даден код може да е злонамерен инструмент за изтегляне, ако:

- има причина да смятаме, че е създаден, за да разпространява PHA, и е изтеглил такива приложения, или съдържа код, който може да изтегля и инсталира приложения; или
- поне 5% от изтеглените чрез него приложения са PHA с минимален праг от 500 наблюдавани изтегляния на приложения (25 наблюдавани изтегляния на PHA).

Основните браузъри и приложения за споделяне на файлове не се смятат за злонамерени инструменти за изтегляне, при условие че:

- не водят до изтегляне без взаимодействие с потребителя; и
- всички изтегляния на PHA са започнати от потребители, които са дали съгласието си.

Заплаха, която не се отнася за Android

Код, съдържащ заплахи, които не се отнасят за Android.

Тези приложения не могат да навредят на потребителя или устройството с Android, но съдържат компоненти, които са потенциално опасни за групи платформи.

Фишинг

Код, за който се твърди, че е от надежден източник, иска идентификационните данни или платежната информация на потребителя и ги изпраща на трета страна. Тази категория се отнася и за програми, които прихващат потребителските идентификационни данни при предаването им.

Някои от най-често срещаните обекти на фишинг атаките са банковите идентификационни данни, номерата на кредитни карти и данните за вход в онлайн профили за социални мрежи и игри.

Злоупотреба с администраторски права

Код, който компрометира целостта на системата чрез пробив в тестовата среда за приложения, получаване на администраторски права или промяна или деактивиране на достъп до основни функции, свързани със сигурността.

Примерите включват:

- Приложения, които нарушават модела за разрешения на Android или крадат идентификационни данни (например означения за OAuth) от други приложения.
- Приложения, които злоупотребяват с функции, за да предотвратят деинсталирането или спирането си.
- Приложения, които деактивират SELinux.

Приложения, които си осигуряват администраторски права и получават пълноправен достъп до устройствата без разрешението на потребителите, се класифицират като приложения за пълноправен достъп.

Рансъмуер

Код, който поема частичен или пълен контрол над устройството или данните му и иска от потребителя да направи плащане или да извърши действие, за да си възвърне контрола.

Някои видове рансъмуер шифроват данните на устройството и изискват плащане, за да ги разшифроват, и/или използват администраторските му функции, така че да предотвратят премахването си от обикновени потребители. Примерите включват:

- Заклучване на устройството и искане на пари за възстановяване на контрола на потребителя.
- Шифроване на данните на устройството и искане на плащане за евентуалното им разшифроване.
- Използване на функциите за управление на правилата за устройството и блокиране на премахването от потребителя.

Разпространяван с устройството код, чиято основна цел е субсидирано управление на устройството, може да бъде изключен от категорията за рансъмуер, при условие че отговаря на критериите за сигурно заключване и управление и на изискванията за разкриване на необходимата информация на потребителите и получаване на съгласие от тях.

Даване на пълноправен достъп

Код, който дава пълноправен достъп до устройството.

Има разлика между злонамерен и незлонамерен код, който дава пълноправен достъп. Например незлонамерените приложения, даващи пълноправен достъп, уведомяват потребителя, че до устройството ще бъде даден пълноправен достъп, и не изпълняват други потенциално опасни действия, които се отнасят за групи категории РНА

Злонамерените приложения, даващи пълноправен достъп до устройството, не уведомяват потребителя за това или пък го правят, но същевременно изпълняват други действия, които се отнасят за групи категории РНА.

Спам

Код, който изпраща нежелани съобщения до контактите на потребителя или използва устройството като средство за разпространение на спам по имейл.

Шпиониращ софтуер

Шпиониращият софтуер е злонамерено приложение, код или действие за събиране, извличане или споделяне на потребителски данни или данни от устройството за цели, които не са свързани със спазващата правилата функционалност.

Злонамереният код и действията, които могат да бъдат сметнати за шпиониране на потребителя или при които се извличат данни без съответното известие или получаване на съгласие, също може да попаднат в категорията за шпиониращ софтуер.

Следват примери за нарушения, категоризирани като шпиониращ софтуер, като списъкът не е изчерпателен:

- записване на аудио или входящи обаждания;
- кражба на данни на приложения;
- приложение със злонамерен код на трета страна (например SDK), който предава данни извън устройството по неочакван за потребителя начин и/или без съответното известие или без съгласието на потребителя.

Приложенията трябва също да спазват всички програмни правила за програмистите в Google Play, включително тези за потребителските данни и данните от устройството, като например правилата относно [нежелания софтуер на мобилни устройства](#), [потребителските данни](#) и [разрешенията и API, които осъществяват достъп до поверителна информация](#), както и [изискванията за SDK](#).

Троянски кон

Код, който изглежда злонамерен – например игра, за която се твърди, че е само игра, но всъщност извършва нежелани действия срещу потребителя.

Тази класификация обикновено се използва в комбинация с други категории за потенциално опасни приложения. Троянският кон съдържа един безобиден и един скрит, опасен компонент. Пример за това е игра, която изпраща платени SMS съобщения от устройството на потребителя на заден план и без негово знание.

Забележка относно необичайните приложения

Възможно е нови и редки приложения да бъдат класифицирани като необичайни, ако Google Play Protect няма достатъчно информация, за да ги определи за безопасни. Това не означава непременно, че дадено приложение е опасно, но за да се потвърди обратното, е необходим допълнителен преглед.

Забележка за категорията „Задни врати“

Класификацията в категорията за злонамерен софтуер със „задна врата“ се основава на поведението на кода. За да бъде дадена програма класифицирана като осигуряваща „задна врата“, тя трябва да позволява поведение, при чиято автоматична проява кодът ще попадне в една от другите категории за злонамерен софтуер. Ако например дадено приложение допуска зареждането на динамичен код за извличане на SMS съобщения, то ще бъде класифицирано като злонамерен софтуер, осигуряващ „задна врата“.

Ако обаче дадено приложение дава възможност за изпълнение на произволен код и нямаме причина да смятаме, че целта на това изпълнение е извършване на злонамерено действие, тогава приложението ще се третира като такова с уязвимост, а не като злонамерен софтуер, осигуряващ „задна врата“, и програмистът ще бъде помолен да го коригира.

Маскуер

Приложение, което използва разнообразни техники за укриване, за да показва на потребителите различна или фалшива функционалност. Тези приложения се маскират като отговарящи на изискванията приложения или игри, за да се показват като безобидни в

магазините с приложения, и използват различни техники, като например маскиране, зареждане на динамичен код или прикриване, за да показват злонамерено съдържание.

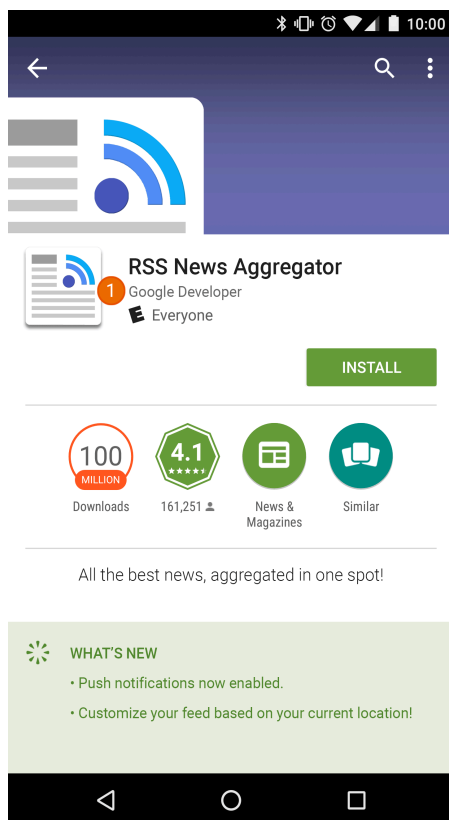
Маскиращият софтуер (маскуер) е подобен на други категории РНА, по-конкретно на троянския кон, като основната разлика е в техниката, използвана за маскиране на злонамерената активност.

Представяне под чужда самоличност

Не допускаме приложения, които подвеждат потребителите, като се представят за друго лице (напр. друг програмист, компания, обект) или приложение. Не създавайте погрешно впечатление, че приложението ви е свързано със или упълномощено от дадено лице. Внимавайте да не използвате икони, описания, заглавия или елементи в приложението, които могат да подвеждат потребителите относно връзката му с друго лице или приложение.

Ето няколко примера за често срещани нарушения:

- Програмисти, които невярно внушават партньорство с друга компания/програмист/юридическо лице/организация.



① Името на програмиста, посочено за това приложение, създава впечатление за официална връзка с Google, въпреки че такава не съществува.

- Приложения, чиито икони и имена невярно внушават партньорство с друга компания/програмист/юридическо лице/организация.

✓		
✗	① 	② 

① Приложението използва национален герб и подвежда потребителите да мислят, че има връзка с правителството.

② Приложението копира логото на даден бизнес, за да внушава невярно, че е официалното му приложение.

- Името и иконите на приложението са толкова подобни на тези на съществуващи продукти или услуги, че потребителите може да бъдат подвеждани.

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

✓	 FISHCOINS	 ATOMIC ROBOT
✗	①  GOLDICOINS	②  ATOMIC ROBOT

① Приложението използва логото на популярен уебсайт за криптовалута в иконата си, за да внушава, че е официалният сайт.

② Приложението копира в иконата си името на известно телевизионно предаване и персонаж от него и подвежда потребителите да мислят, че има връзка с предаването.

- Приложения, за които невярно се твърди, че са официалното приложение на определен субект. Имена като Justin Bieber Official не са позволени без необходимите разрешения или права.
- Приложения, които нарушават [указанията за марката Android](#).

Нежелан софтуер на мобилни устройства

В Google смятаме, че ако се съсредоточим върху нуждите на потребителя, всичко останало ще последва само. В нашите [принципи относно софтуера](#) и [правила относно нежелания софтуер](#) предоставяме общи препоръки за софтуера, които осигуряват отлична

практическа работа на потребителите. Тези правила се основават на правилата ни относно нежелания софтуер, като очертават принципите за [екосистемата на Android](#) и Google Play Магазин. Софтуерът, който нарушава тези принципи, е потенциално опасен за потребителите и ще предприемем стъпки, за да ги защитим от него.

Както споменахме в [правилата относно нежелания софтуер](#), установихме, че по-голямата част от този тип софтуер демонстрира една или повече от същите основни характеристики:

- Подвежда потребителите с предложение за стойност, което не се изпълнява;
- Опитва да подмами потребителите да го инсталират или се инсталира заедно с друга програма;
- Не информира потребителя относно всичките си главни и значими функции;
- Засяга системата на потребителя по неочаквани начини;
- Събира или предава поверителна информация без знанието на потребителите;
- Събира или предава поверителна информация, без да я обработва по надежден начин (напр. предаване през HTTPS);
- Предлага се в пакет с друг софтуер, без това да е упоменато.

На мобилни устройства софтуерът представлява код под формата на приложение, двоичен код, промяна в софтуерната рамка и др. За да не допуснем софтуер, който е опасен за екосистемата или нарушава практическата работа на потребителите, ще предприемем действия спрямо всеки код, който нарушава тези принципи.

По-долу използваме правилата относно нежелания софтуер, за да разширим приложимостта им за мобилен софтуер. Ще продължим да подобряваме и тях, и правилата относно нежелания софтуер за мобилни устройства, така че да обхващат нови типове злоупотреби.

Прозрачно поведение и разкриване по ясен начин

Всеки код трябва да изпълнява дадените на потребителя обещания. Приложенията трябва да осигуряват всички обявени функционалности. Приложенията не трябва да объркват потребителите.

- Приложенията трябва да посочват ясно функциите и целите.
- Обяснете на потребителите изрично и ясно какви системни промени ще бъдат извършени от приложението. Дайте им възможност да преглеждат и одобряват всички значими опции за инсталиране и промени.
- Софтуерът не трябва да създава подвеждаща представа за състоянието на устройството на потребителя, например да твърди, че системата е в критично състояние на сигурността или е заразена с вируси.
- Не използвайте невалидна активност, предназначена да увеличи рекламния трафик и/или реализациите.
- Не допускаме приложения, които подвеждат потребителите, като се представят за друго лице (напр. друг програмист, компания, обект) или приложение. Не създавайте погрешно впечатление, че приложението ви е свързано със или упълномощено от дадено лице.

Примери за нарушения:

- измама с реклами;
- социално инженерство.

Защита на потребителските данни и поверителността

Осигурете яснота и прозрачност по отношение на достъпа, използването, събирането и споделянето на лични и чувствителни потребителски данни. При използване на потребителски данни трябва да се спазват съответните правила, където е приложимо, и да се вземат всички предпазни мерки за защита на данните.

Приложенията трябва да спазват всички програмни правила за програмистите в Google Play, включително тези за потребителските данни и данните от устройството, като например правилата относно [потребителските данни](#), [разрешенията и API](#), [които осъществяват достъп до поверителна информация](#), [шпиониращия софтуер](#), както и [изискванията за SDK](#).

- Не искайте и не подвеждайте потребителите да изключат механизмите за защита на устройството, като например Google Play Protect. Например не бива да предлагате на потребителите допълнителни функции или награди в приложението, за да изключат Google Play Protect.

Не смуцавайте практическата работа на мобилни устройства

Практическата работа на потребителите трябва да е недвусмислена, лесна за разбиране и въз основа на взетите от тях решения, за които са имали ясни възможности за избор. Тя трябва да представя ясно стойностно предложение на потребителя и да не пречи на рекламираната или желаната практическа работа.

- Не показвайте реклами на потребителите по неочаквани начини, включително такива, които влошават или възпрепятстват използваемостта на функциите на устройството. Не трябва да използвате и реклами, които се показват извън средата на задействащото приложение, ако не могат да се отхвърлят лесно и ако нямат подходящо съобщение за получаване на съгласие и означение за авторство.
- Приложенията не трябва да пречат на други приложения, нито на използваемостта на устройството.
- Опцията за деинсталиране, където е приложимо, трябва да е ясно посочена.
- Мобилният софтуер не трябва да имитира подкани от операционната система на устройството или от други приложения. Не блокирайте сигнали до потребителя от други приложения или от операционната система, особено такива, които го информират за промени в операционната система.

Примери за нарушения:

- натрапчиви реклами;
- неупълномощено използване или имитиране на системна функционалност.

Злонамерени инструменти за изтегляне

Код, който сам по себе си не е нежелан софтуер, но изтегля друг нежелан софтуер за мобилни устройства (MUwS).

Даден код може да е злонамерен инструмент за изтегляне, ако:

- има причина да смятаме, че е създаден, за да разпространява MUwS, и е изтеглил такива приложения, или съдържа код, който може да изтегля и инсталира приложения; или
- поне 5% от изтеглените чрез него приложения са MUwS с минимален праг от 500 наблюдавани изтегляния на приложения (25 наблюдавани изтегляния на MUwS).

Основните браузъри и приложения за споделяне на файлове не се смятат за злонамерени инструменти за изтегляне, при условие че:

- не водят до изтегляне без взаимодействие с потребителя; и
- всички изтегляния на софтуер са започнати от потребители, които са дали съгласието си.

Измама с реклами

Измамата с реклами е строго забранена. Взаимодействията с реклами, генерирани с цел рекламна мрежа да бъде подведена, че трафикът е от реален потребителски интерес, представляват измама с реклами, която е форма на [невалиден трафик](#). Измамата с реклами

може да е допълнителен резултат от внедряването на реклами от програмистите по непозволен начини, например показване на скрити реклами, автоматично кликване върху реклами, промяна или преправяне на информация и възползване по друг начин от действия, които не се извършват от хора (паяци, роботи и др.), или човешки дейности с цел да се генерира невалиден рекламен трафик. Невалидният трафик и измамата с реклами са вредни за рекламодателите, програмистите и потребителите и водят до дългосрочна загуба на доверие в екосистемата на мобилните реклами.

Ето няколко примера за често срещани нарушения:

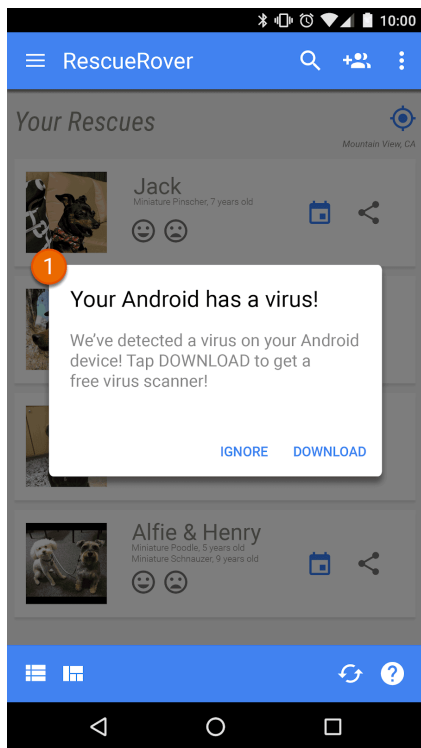
- Приложение, изобразяващо реклами, които не се виждат от потребителя.
 - Приложение, което автоматично генерира кликвания върху реклами, без потребителят да е имал такова намерение, или което генерира еквивалентен трафик в мрежата, за да приписва кредити за кликвания по измамнически начин.
 - Приложение, което изпраща фалшиви кликвания за приписване на инсталиране, за да получи плащане за инсталирания, които не идват от мрежата на подателя.
 - Приложение, което показва реклами в изскачащи прозорци, когато потребителят не е в интерфейса му.
 - Невярно представяне на рекламните места от приложение, например такова, което съобщава на рекламните мрежи, че се изпълнява на устройство с iOS, а в действителност работи на устройство с Android. Приложение, което представя по подвеждащ начин името на пакета, от който се осигуряват приходи.
-

Неупълномощено използване или имитиране на системна функционалност

Не допускаме приложения или реклами, които имитират или възпрепятстват системна функционалност, като например известия или предупреждения. Известията на ниво система може да се използват само за функции, които са неразделна част от съответния продукт, например приложение на авиокомпания, което уведомява потребителите за специални оферти, или игра, която ги уведомява за промоции в нея.

Ето няколко примера за често срещани нарушения:

- Приложения или реклами, които се показват чрез системно известие или сигнал:



① Показването в това приложение системно известие се използва за извеждане на реклама.

За допълнителни примери относно рекламите направете справка със [съответните правила](#).

Социално инженерство

Не допускаме приложения, които се представят за други такива с цел да подведат потребителите, така че те да извършат действия, предназначени за първоначалното доверено приложение.

Осигуряване на приходи и реклами

В полза на програмистите и потребителите Google Play поддържа редица стратегии за осигуряване на приходи, включително платено разпространение, продукти в приложения, абонаменти, както и модели, основани на реклами. За да се гарантира възможно най-добра работа на потребителите, трябва да спазвате тези правила.

Плащания

1. Програмистите, които таксуват за изтегляния на приложения от Google Play, трябва да използват като начин на плащане за тези транзакции съответната система в услугата.
2. Приложенията, разпространявани чрез Google Play, които изискват или приемат плащания за достъп до функции или услуги в приложението, включително функционалности на приложението, дигитално съдържание или стоки (наричани събирателно „покупки в приложение“), трябва да използват системата на Google Play за таксуване за тези транзакции, освен ако не е приложима секция 3, 8 или 9.

Примерите за функции или услуги в приложението, които изискват използването на системата на Google Play за таксуване, включват, но не се ограничават до, следните покупки в приложението:

- елементи (като например виртуални валути, допълнителни животи, допълнително време за игра, добавки, герои и аватари);
- абонаментни услуги (например за фитнес, игри, запознанства, образование, музика, видеоклипове, актуализации на услуги и друго съдържание);
- функционалност или съдържание в приложение (като например версия без реклами или нови функции, които не са налични в безплатната версия);
- софтуер и услуги в облак (като например услуги за съхранение на данни, софтуер за бизнес производителност, както и такъв за финансово управление).

3. Системата на Google Play за таксуване не трябва да се използва в случаите, когато:

а. плащането е преди всичко за:

- покупка или наемане на физически стоки (като например хранителни продукти, грехи, домашни потреби и електроника);
- покупка на физически услуги (като например транспортни услуги, почистване, членство във фитнес, доставка на храна, самолетни билети и такива за събития на живо);
- превод на сума във връзка със сметка по кредитна карта или такава за комунални услуги (като например кабелни и телекомуникационни услуги);

б. плащанията включват директни плащания от един до друг потребител, онлайн търгове и освободени от данъци дарения;

с. плащането е за съдържание или услуги, които улесняват онлайн хазарта, както е описано в секцията [Приложения за хазарт](#) на [правилата за хазарт, игри и състезания с истински пари](#);

д. плащането е свързано с категория продукти, която се смята за неприемлива съгласно [правилата за съдържанието в Центъра ни за плащания](#) .

Забележка: За някои пазари предлагаме Google Pay за приложения, в които се продават физически стоки и/или услуги. За повече информация посетете съответната ни [страница за програмисти](#) .

4. Освен при условията, описани в секция 3, секция 8 и секция 9, приложенията не могат да отвеждат потребителите до начин на плащане, различен от системата на Google Play за таксуване. Тази забрана включва, без изброяването да е изчерпателно, отвеждането на потребителите до други начини на плащане чрез:

- малката обява в Google Play за приложението;
- промоции в приложението, свързани със съдържание, което може да се купи;
- изгледи в мрежата, бутони, връзки, съобщения, реклами или други подканващи фрази в приложението;
- процедури с потребителския интерфейс на приложението, включително такива за създаване на профил или регистрация, в хода на които потребителите биват отвеждани от приложението до начин на плащане, различен от системата на Google Play за таксуване.

5. Виртуалните валути трябва да се използват само в рамките на приложението, в което са закупени първоначално.

6. Програмистите трябва ясно и точно да информират потребителите за условията и цените на приложението си, както и за всички предлагани за покупка функции или абонаменти в него. Цените в приложението трябва да съответстват на показаните на потребителите в интерфейса на Play Billing. Ако информацията в описанието в Google Play се отнася за функции в приложение, за които може да се изисква определено или

допълнително таксуване, в малката обява трябва да е ясно упоменато, че за достъп до тях се изисква плащане.

7. Приложенията и игрите, които предлагат механизми за получаване на определени по рандомизиран начин виртуални елементи от дадена покупка, включително, но не само, купии с награди, трябва ясно да разкрият вероятността за получаването им преди покупката и в близък до нея момент.
8. Освен ако не са приложими условията, описани в секция 3, програмистите на разпространявани чрез Google Play приложения, които изискват или приемат плащания от потребители в тези [гържави/региони](#) за достъп до покупки в приложението, може да предлагат на потребителите система за алтернативно таксуване в приложението в допълнение към системата на Google Play за таксуване за тези транзакции, ако попълнят успешно формуляра за деклариране за таксуване за съответната програма и приемат включените в него допълнителни условия и [програмни изисквания](#).
9. Програмистите на разпространявани чрез Google Play приложения могат да отвеждат потребителите в Европейското икономическо пространство (ЕИП) извън приложението, включително, за да популяризират оферти за дигитални функции и услуги в приложенията. Програмистите, които отвеждат потребителите в ЕИП извън приложението, трябва да попълнят успешно [формуляра за деклариране](#) за съответната програма и да приемат включените в него допълнителни условия и [програмни изисквания](#).

Забележка: За да прегледате хронологията и често задавани въпроси относно тези правила, моля, посетете [Помощния ни център](#).

Реклами

За да поддържаме качествена практическа работа, вземаме предвид съдържанието, аудиторията, практическа работа на потребителите и поведението на рекламата ви, както и сигурността и поверителността. Смятаме рекламите и свързаните с тях оферти за част от приложението ви. Те трябва да спазват и всички други правила на Google Play. Освен това имаме допълнителни изисквания за рекламите, ако си осигурявате приходи от приложение, насочено към деца в Google Play.

Също така [мык](#) можете да прочетете повече за правилата ни относно малките обяви в магазина и популяризирането на приложения, включително какво предприемаме по отношение на [подвеждащите практики за популяризиране](#).

Рекламно съдържание

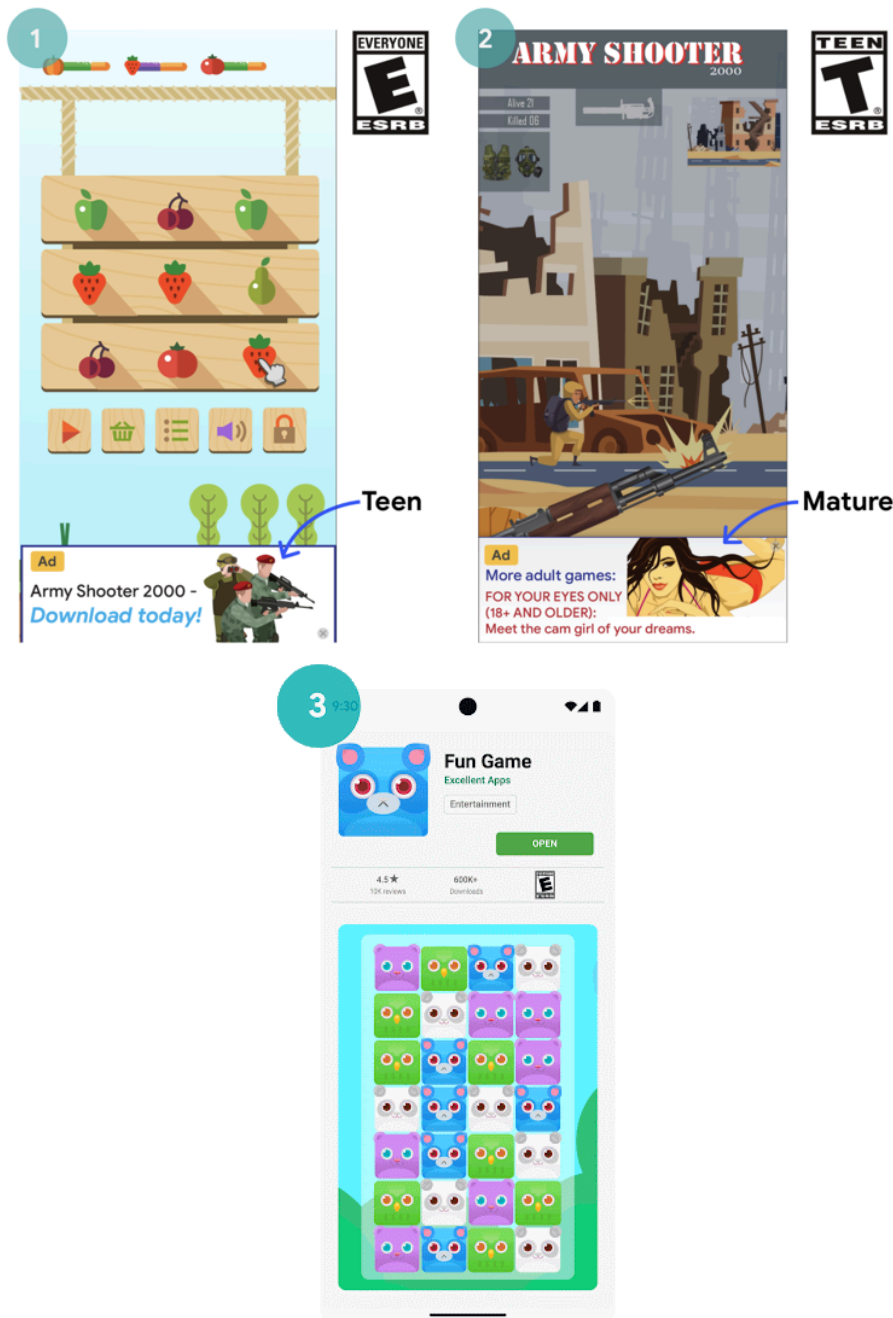
Рекламите и свързаните с тях оферти са част от приложението ви и трябва да спазват правилата ни относно [ограниченото съдържание](#). Ако приложението ви е за [хазарт](#), са в сила допълнителни изисквания.

Неподходящи реклами

Рекламите и свързаните с тях оферти (например рекламата популяризира изтеглянето на друго приложение), показвани в приложението ви, трябва да са подходящи за [класификацията на съдържанието](#) му, дори съдържанието им само по себе си да спазва правилата ни.

Ето няколко примера за често срещани нарушения:

- Реклами, които не са подходящи за класификацията на съдържанието на приложението:



- ① Тази реклама (за тийнейджъри) не е подходяща за класификацията на съдържанието на приложението (за всички възрасти)
- ② Тази реклама (за пълнолетни) не е подходяща за класификацията на съдържанието на приложението (за тийнейджъри)
- ③ Офертата на рекламата (популяризиране на изтеглянето на приложение за пълнолетни) не е подходяща за класификацията на съдържанието на приложението за игра, където е била показана рекламата (за всички възрасти)

Изисквания за рекламите за семейства

Ако си осигурявате приходи от приложение, насочено към деца в Google Play, е важно то да изпълнява изискванията на [правилата относно рекламите за семейства и осигуряването на приходи](#).

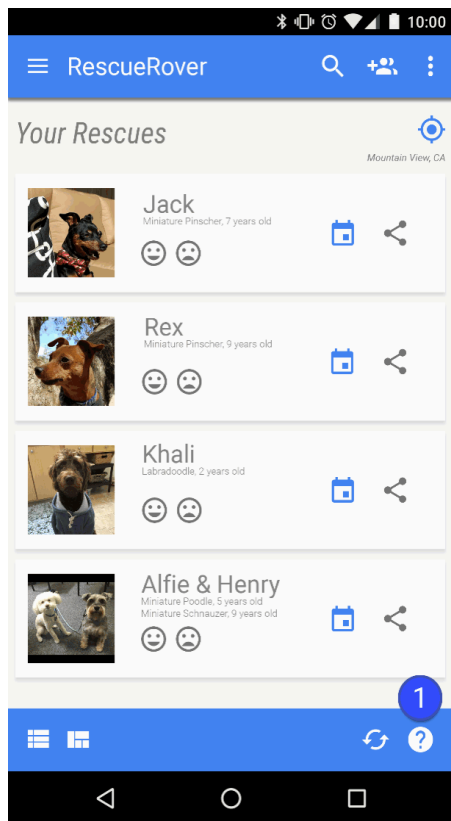
Подвеждащи реклами

Рекламите не трябва да имитират или да се представят за потребителския интерфейс на някоя функция на приложение, като например известия, нито за предупреждения от

операционната система. Потребителят трябва да е наясно от кое приложение се показва всяка реклама.

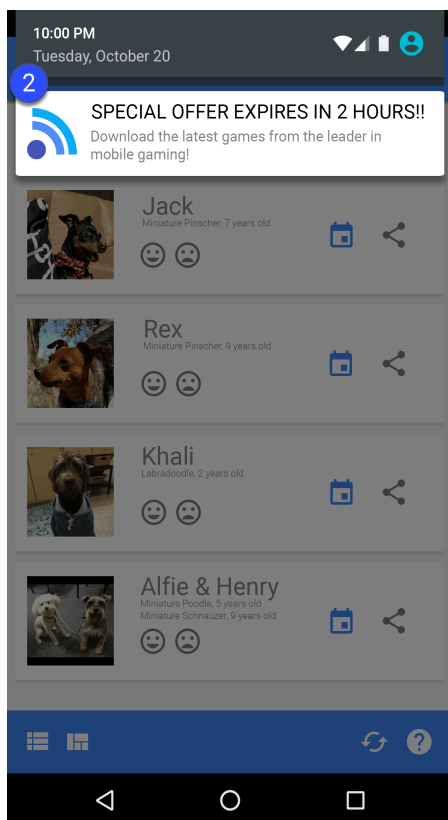
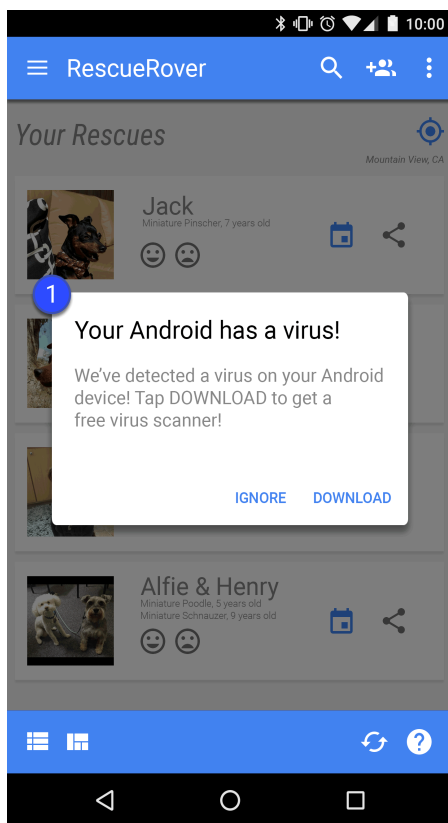
Ето няколко примера за често срещани нарушения:

- Реклами, които имитират потребителския интерфейс на приложение:

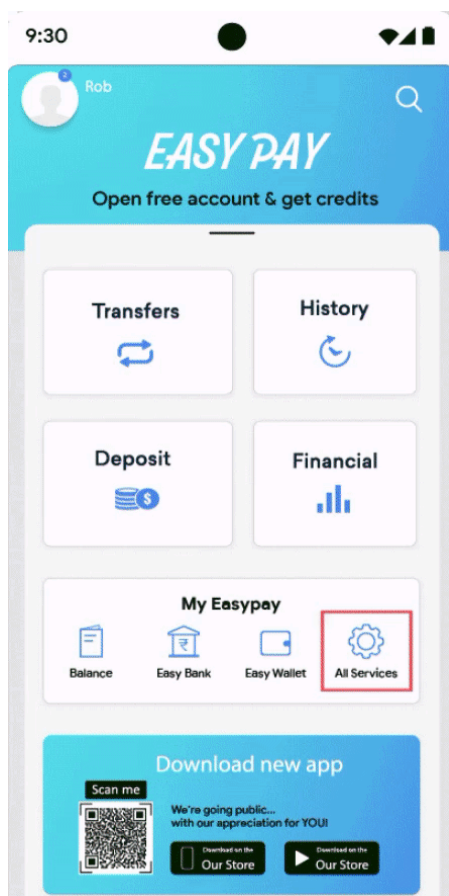


① Иконата на въпросителен знак в това приложение е реклама, която отвежда потребителя до външна целева страница.

- Реклами, които имитират системно известие:



① ② В примерите по-горе са показани реклами, които имитират различни системни известия.



① Примерът по-горе показва секция с функции, която имитира други функции, но води потребителя само до реклама или реклами.

Натрапчиви реклами

Натрапчивите реклами се показват на потребителите по неочаквани начини, които могат да доведат до непреднамерени кликания или които влошават или възпрепятстват използваемостта на функциите на устройството.

Приложението ви не може да принуждава потребителя да кликне върху реклама или да изпрати лична информация за рекламни цели, за да може да се възползва от пълната функционалност на приложението. Рекламите може да се показват само в приложението, от което произлизат, и не трябва да пречат на други приложения и реклами, нито на работата на устройството, в това число системни или физически бутони и портове. Това включва наслагвания, придружаващи функционалности или рекламни елементи под формата на приспособления. Ако в приложението ви се извеждат реклами, които възпрепятстват нормалното му използване, те трябва да могат да се отхвърлят лесно, без отрицателни последици за потребителите.

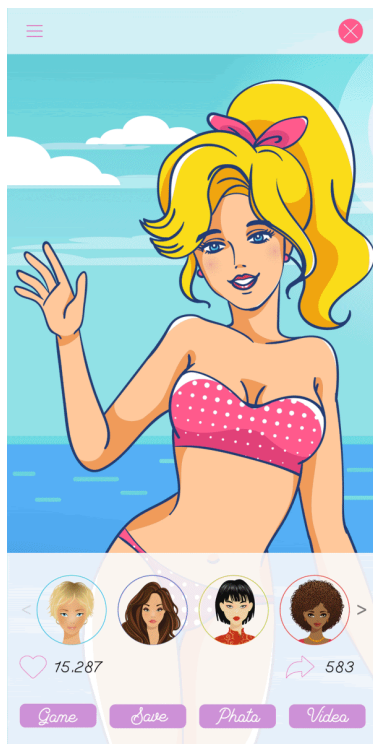
Ето няколко примера за често срещани нарушения:

- Реклами, които заемат целия екран или възпрепятстват нормалното използване и не предоставят ясен начин за отхвърлянето си:

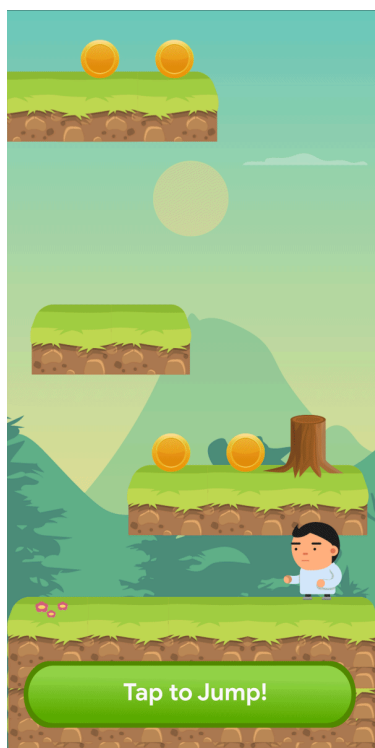


① Тази реклама няма бутон за отхвърляне.

- Реклами, които принуждават потребителя да кликне върху тях, като използват лъжлив бутон за отхвърляне, или се показват внезапно в части от приложението, където потребителят обикновено докосва, за да използва друга функция:

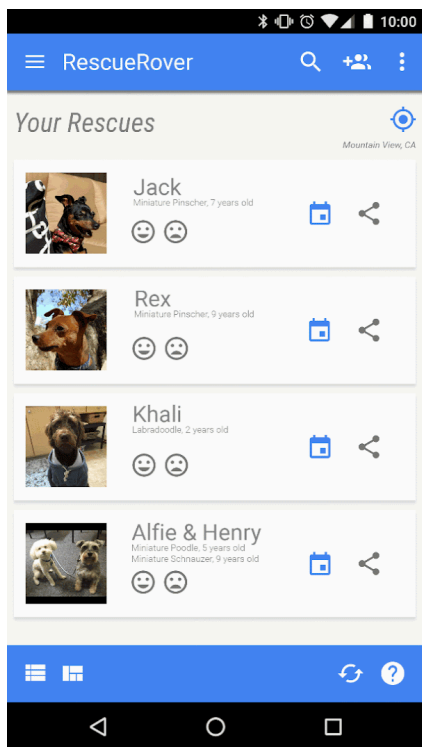


① Тази реклама използва лъжлив бутон за отхвърляне.



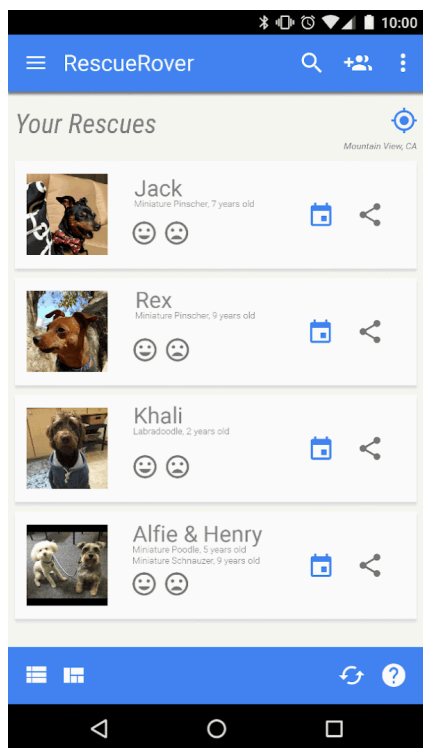
② Тази реклама внезапно се показва в област, където потребителят е свикнал да докосва, за да използва функции в приложението.

- Реклами, показвани извън приложението, от което произлизат:



① Докато използва това приложение, потребителят преминава към началния екран и там внезапно се показва реклама.

- Реклами, които се задействат с бутона „Начало“ или чрез други функции, изрично предназначени за изход от приложението:



① Потребителят опитва да излезе от приложението и да стигне до началния екран, но вместо това се показва реклама.

Практическа работа със „Стандарти за по-добри реклами“

Програмистите трябва да спазват следните указания за рекламите, за да гарантират висококачествена практическа работа за потребителите, когато те използват приложения от Google Play. Рекламите ви не могат да се показват на потребителите по следните неочаквани начини:

- Не се допускат рекламни заставки на цял екран в какъвто и да е формат (видео, GIF, статични и др.), които се показват неочаквано, обикновено когато потребителят е избрал да направи нещо друго.
- Не се допускат реклами по време на игра в началото на ниво или в началото на сегмент от съдържанието.
- Не се допускат рекламни видеозаставки на цял екран, които се показват преди екрана за зареждане (първоначалния екран).
- Не се допускат рекламни заставки на цял екран в какъвто и да е формат, които не могат да бъдат затворени след 15 секунди. Рекламни заставки на цял екран, които дават възможност за избор или които не прекъсват действията на потребителите (например след екрана с резултата в приложение за игра), може да се задържат повече от 15 секунди.

Това правило не се прилага за реклами с поощрение, за които потребителите изрично са се включили (например реклама, която програмистите изрично предлагат на даден потребител, за да я гледа в замяна на отключването на конкретна функция в играта или определено съдържание). Това правило не се прилага и за осигуряването на приходи и рекламите, които не възпрепятстват обичайното използване на приложението или начина на игра (например видеосъдържание с интегрирани реклами и банерни реклами, които не са на цял екран).

Тези указания са вдъхновени от [Стандарти за по-добри реклами – практическа работа с мобилни приложения](#). За повече информация относно „Стандарти за по-добри реклами“ направете справка с [Коалицията за по-добри реклами](#).

Ето няколко примера за често срещани нарушения:

- Неочаквани реклами, които се показват по време на игра или в началото на сегмент от съдържанието (например след като потребител е кликнал върху бутон и преди очакваното действие от кликването да бъде извършено). Тези реклами са неочаквани, тъй като вместо тях потребителите очакват да започнат игра или да се ангажират със съдържание.

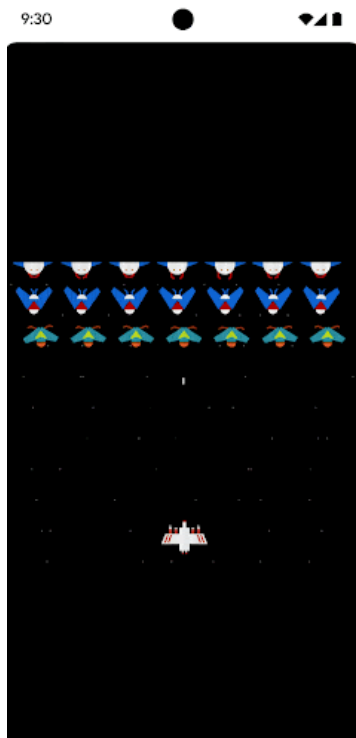


① Неочаквана статична реклама се показва по време на игра в началото на дадено ниво.



② Неочаквана видеореклама се показва в началото на сегмент от съдържанието.

- Реклама на цял екран, която се показва по време на игра и не може да бъде затворена след 15 секунди.



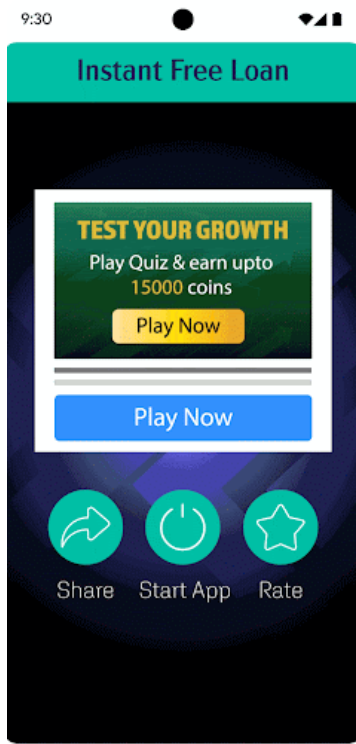
① Рекламна заставка се показва по време на игра и не предлага на потребителя опция за пропускане в рамките на 15 секунди.

Рекламно предназначение

Не допускаме приложения, които многократно показват рекламни заставки, за да разсейват потребителите, пречейки им да взаимодействат с приложението или да изпълняват задачи в него.

Ето няколко примера за често срещани нарушения:

- Приложения, в които рекламна заставка се показва непрекъснато след действие на потребителя (включително, но не само, кликване, прекарване на пръст и др.).



① Първата страница в приложението има множество бутони, с които да се взаимодейства. Когато потребителят задейства **Start app**, за да използва приложението, изскача рекламна заставка. След затваряне на рекламата потребителят се връща в приложението и кликва върху **Service**, за да започне да използва услугата, но се показва друга рекламна заставка.

② На първата страница потребителят е заставен да кликне върху **Play**, тъй като това е единственият наличен бутон, за да използва приложението. Когато потребителят кликне върху него, се показва рекламна заставка. След затваряне на рекламата потребителят кликва върху **Launch**, тъй като това е единственият бутон, с който може да взаимодейства, и изскача друга рекламна заставка.

Осигуряване на приходи от заключения екран

Освен ако изключителната цел на приложението не е да представлява заключен екран, то няма право да съдържа реклами или функции, които служат за осигуряване на приходи от заключения екран на устройството.

Измама с реклами

Измата с реклами е строго забранена. За повече информация разгледайте [правилата ни относно измамите с реклами](#).

Използване на данни за местоположението за реклами

Приложенията, при които употребата на данните за местоположението на устройството въз основа на разрешения се разширява до показване на реклами, се обхващат от правилата за [личната и поверителната информация](#) и трябва също така да изпълняват следните изисквания:

- Използването или събирането на данни за местоположението на устройството въз основа на разрешения с цел рекламиране трябва да бъде ясно за потребителя и да е документирано в задължителната декларация за поверителност на приложението, включително чрез посочване на връзки към декларациите за поверителност на съответните рекламни мрежи, в които се обхваща използването на данни за местоположението.
- В съответствие с изискванията за [разрешенията за достъп до местоположението](#) тези разрешения може да се искат само с цел реализиране на текущи функции или услуги в приложението ви, като нямате право да искате разрешения за достъп до местоположението на устройството единствено с цел рекламиране.

Използване на идентификатора за рекламиране за Android

Версия 4.0 на услугите за Google Play представи нови приложни програмни интерфейси (API) и идентификатор, които да се използват от доставчиците на реклами и решения за анализ. Следват условията за употребата на този идентификатор.

- **Употреба.** Идентификаторът за рекламиране за Android трябва да се използва само за рекламиране и потребителски анализ. Състоянието на настройката за отказване от рекламирането въз основа на интереси или отказване от персонализиране на рекламите трябва да се проверява при всяко осъществяване на достъп до идентификатора.
- **Свързване с информация, позволяваща лично идентифициране, или други идентификатори.**
 - Използване за рекламна цел: Идентификаторът за рекламиране не може да се свързва с постоянни идентификатори на устройството (например SSAID, MAC адрес, IMEI и др.) за

каквито и да е рекламни цели. Той може да се свързва с позволяваща лично идентифициране информация само с изричното съгласие на потребителя.

- Използване с цел анализ: Идентификаторът за рекламиране не може да се свързва с информация, позволяваща лично идентифициране, или с постоянни идентификатори на устройството (например SSAID, MAC адрес, IMEI и др.) с цел анализ. За допълнителни указания относно постоянните идентификатори на устройството, моля, прочетете [правилата за потребителските данни](#).
- **Зачитане на избора на потребителите.**
 - При повторно задаване новият идентификатор за рекламиране не трябва да се свързва с предишен такъв или с извлечени от него данни без изричното съгласие на потребителя.
 - Трябва да спазвате зададената от потребителя настройка за отказване от рекламирането въз основа на интереси или отказване от персонализиране на рекламите. Ако тя е активирана, нямате право да използвате идентификатора за рекламиране, за да създавате потребителски профили за рекламни цели или да насочвате персонализирани реклами към потребителите. Разрешените дейности включват контекстно рекламиране, ограничаване на честотата, проследяване на реализациите, отчитане, защита и откриване на измами.
 - На по-новите устройства, когато потребител изтрие идентификатора за рекламиране в Android, идентификаторът ще бъде премахнат. Ако потребителят се опита да осъществи достъп до идентификатора, вместо него ще види поредица от нули. Ако дадено устройство няма идентификатор за рекламиране, то не трябва да бъде свързвано с данни, произлизащи от предишен идентификатор за рекламиране или свързани с такъв.
- **Прозрачност за потребителите.** Извличането и използването на идентификатора за рекламиране, както и обвързването с тези условия трябва да бъдат разкрити на потребителите в юридически издържано съобщение за поверителност. За да научите повече за стандартите ни за поверителност, моля, прегледайте правилата ни за [потребителските данни](#).
- **Спазване на Общите условия.** Идентификаторът за рекламиране може да се използва само съгласно програмните правила за програмистите в Google Play, включително от всяка страна, с която е възможно да го споделите при обичайната си бизнес дейност. Всички приложения, качени или публикувани в Google Play, трябва да ползват за всякакви рекламни цели този идентификатор (когато е налице на устройството) вместо каквито и да е други идентификатори на устройството.

За повече информация разгледайте [правилата ни за потребителските данни](#).

Абонаменти

Като програмист не трябва да подвеждате потребителите за абонаментните услуги или съдържанието, които предлагате в приложението си. Важно е те да са ясно описани във всички популяризации в приложението или на първоначалните екрани. Не допускаме приложения, които подлагат потребителите на измамна или манипулативна практическа работа при покупка (включително покупки в приложението или абонаменти).

Офертите ви трябва да бъдат прозрачни. Това включва подробно описание на условията на офертата, цената на абонамента, честотата на цикъла на таксуване и дали за използване на приложението се изисква абонамент. Потребителите не трябва да извършват допълнително действие, за да прегледат информацията.

Абонаментите трябва да предлагат на потребителите непрекъсната или повтаряща се стойност през съответния период. Абонаментите не могат да се използват, за да предлагате на потребителите еднократни предимства (например складови единици на продукт, предоставящи голямо количество кредит/валута в играта или еднократни игрови

поощрения). Абонаментът ви може да предлага стимул или промоционални бонуси, но те трябва да са в допълнение към непрекъснатата или повтарящата се стойност през съответния период. Продуктите, които не предлагат непрекъсната или повтаряща се стойност, трябва да използват [продукт в приложение](#) вместо [такъв с абонамент](#).

Не бива да прикривате или погрешно да характеризирате еднократните предимства като абонаменти. Това включва промяната на даден абонамент с цел да бъде превърнат в еднократно предложение (например анулиране, оттегляне или свеждане до минимум на повтарящата се стойност), след като потребителят е купил абонамента.

Ето няколко примера за често срещани нарушения:

- Месечни абонаменти, за които потребителите не получават информация, че се подновяват автоматично и таксуването е всеки месец.
- Годишни абонаменти, в които се изтъква месечната цена.
- Цени и условия на абонамента, които не са изцяло локализирани.
- Популяризации в приложението, които не показват ясно, че потребителят има достъп до съдържание без абонамент (когато е налице).
- Имена на складови единици на продукт, които не предават правилно естеството на абонамента, като например „Пробен период без парично заплащане“ или „Изпробвайте членство в Premium – без парично заплащане за 3 дни“ за абонамент с автоматично периодично таксуване.
- Няколко екрана в потока за покупка, които карат потребителите случайно да кликнат върху бутона за абонамент.
- Абонаменти, които не предлагат непрекъсната или повтаряща се стойност — например такива, които предоставят 1000 скъпоценни камъка за първия месец, след което предимството намалява до 1 скъпоценен камък за следващите месеци от абонамента.
- Потребителят трябва да се регистрира за абонамент, който се подновява автоматично, за да доставите еднократно предимство, след което да анулирате закупения от потребителя абонамент, без да сте получили заявка за това.

Пример 1:

- ① Бутонът за отхвърляне не се вижда ясно и е възможно потребителите да не разберат, че имат достъп до определена функционалност, без да приемат офертата за абонамент.
- ② Офертата показва само месечната цена и е възможно потребителите да не разберат, че ще бъдат таксувани с цената за шест месеца, когато се абонират.
- ③ Офертата показва само промоционалната цена при въвеждане и е възможно потребителите да не разберат с каква сума ще бъдат таксувани автоматично в края на промоционалния период.
- ④ Офертата трябва да е локализирана на същия език като общите условия, така че потребителите да могат да разберат всичко.

Пример 2:

- ① Повтарящите се кликания върху бутон на едно и също място карат потребителя непреднамерено да натисне последния бутон „Напред“, за да се абонира.
- ② Сумата, с която потребителите ще бъдат таксувани след края на пробния период, се разчита трудно, така че потребителите могат да помислят, че планът се предлага без парично заплащане.

Оферти за безплатен пробен период и за промоционална цена при въвеждане

Преди даден потребител да се регистрира за абонамента ви: Трябва ясно и точно да посочите условията на офертата си, включително продължителността, цената и описанието на достъпното съдържание или услуги. Не забравяйте да уведомите потребителите как и кога даден безплатен пробен период преминава в платен абонамент, колко ще струва той и че може да бъде анулиран, ако потребителят не желае да премине към него.

Ето няколко примера за често срещани нарушения:

- Оферти, в които не е ясно посочено каква е продължителността на безплатния пробен период или на промоционалната цена при въвеждане.
- Оферти, в които не е ясно посочено, че потребителят ще бъде автоматично регистриран за платен абонамент в края на периода на офертата.
- Оферти, в които не е ясно посочено, че потребителят може да осъществява достъп до съдържанието и без пробен период (когато това е налице).
- Цената и условията на офертата не са изцяло локализирани.

- ① Бутонът за отхвърляне не се вижда ясно и е възможно потребителите да не разберат, че имат достъп до определена функционалност, без да се регистрират за безплатния пробен период.
- ② В офертата се набляга на безплатния пробен период и е възможно потребителите да не разберат, че ще бъдат таксувани автоматично в края му.
- ③ В офертата не се споменава пробен период и е възможно потребителите да не разберат колко дълго ще имат безплатен достъп до абонаментното съдържание.
- ④ Офертата трябва да е локализирана на същия език като общите условия, така че потребителите да могат да разберат всичко.

Управление и анулиране на абонаменти и възстановяване на суми за тях

Ако продавате абонаменти в приложенията си, трябва да разкриете по ясен начин в тях как даден потребител може да управлява или да анулира абонамента си. Също така трябва да включите в приложението си достъп до лесен за използване онлайн начин за анулиране на абонамента. В настройките на профила в приложението (или еквивалентна страница) можете да изпълните това изискване, като включите:

- Връзка към центъра на Google Play за абонаменти (за приложения, които използват системата ни за таксуване); и/или
- директен достъп до процедурата си за анулиране.

При анулиране на абонамент, купен чрез системата на Google Play за таксуване, според общите ни правила няма да възстановим сумата за текущия период на фактуриране, но потребителят ще продължи да получава абонаментното съдържание за оставащата част от периода независимо от датата на анулиране. Абонаментът ще бъде прекратен след края на текущия период на фактуриране.

В качеството си на доставчик на съдържанието или достъпа имате право непосредствено да реализирате за потребителите си по-гъвкави правила за възстановяване на средства. Ваше задължение е да уведомявате потребителите за промените в правилата си за

абонаментите, анулирането и възстановяването на средства и да се грижите правилата да спазват приложимото законодателство.

Програма за самостоятелно сертифицирани SDK за реклами за семейства

Ако показвате реклами в приложението си и целевата му аудитория включва единствено деца съгласно описаното в [правилата за семейства](#), трябва да използвате само версии на SDK за реклами, които са самостоятелно сертифицирани за това, че спазват правилата на Google Play, включително голупосочените изисквания за самостоятелно сертифицираните SDK за реклами за семейства.

В случай че приложението е насочено както към деца, така и към по-възрастни потребители, трябва да се погрижите рекламите за деца да се показват само от самостоятелно сертифицирани версии на SDK за реклами (например чрез неутрално отсяване по възраст).

Имайте предвид, че вие имате задължението всички версии на SDK, които внедрите в приложението си, включително самостоятелно сертифицираните версии на SDK за реклами, да спазват всички приложими правила, местни закони и разпоредби. Google не прави никакви твърдения и не дава гаранции относно точността на информацията, която SDK за реклами предоставя по време на процеса на самостоятелно сертифициране.

Използването на самостоятелно сертифицирани SDK за реклами за семейства се изисква само ако ползвате SDK за реклами, за да показвате реклами на деца. Следните начини на употреба са разрешени, без да се изисква самостоятелно сертифициране на SDK за реклами в Google Play. Ваша отговорност е обаче практиките ви за рекламно съдържание и събиране на данни да спазват [правилата за потребителските данни](#) и [правилата за семейства](#) на Google Play:

- собствено рекламиране, при което използвате SDK, за да управлявате крос-медийно популяризиране на приложенията си или други притежавани от вас медии и стоки;
- сключване на директни сделки с рекламодатели, при които използвате SDK за управление на рекламните места.

Изисквания за самостоятелно сертифицираните SDK за реклами за семейства

- Дефинирайте нежелателното рекламно съдържание и поведение и ги забранете в общите условия или правилата на SDK за реклами. Дефинициите трябва да спазват програмните правила за програмистите в Google Play.
- Създайте метод за класифициране на рекламните си послания според възрастовите групи, за които са подходящи. Групите трябва да включват поне „За всички възрасти“ и „За пълнолетни“. Методологията за класифициране трябва да съответства на тази, която Google предоставя на SDK, след като програмистите са попълнили формуляра за предявяване на интерес по-долу.
- Разрешете на издателите да поискат (въз основа на заявка или за отделно приложение) показваните реклами да се третираят като предназначени за деца. Третирането им по този начин трябва да спазва приложимите закони и разпоредби, като например [Закона за защита на личната неприкосновеност на децата онлайн \(COPPA\) в САЩ](#) и [Общия регламент относно защитата на данните \(ОРЗД\) в ЕС](#). Като част от третирането на рекламите като предназначени за деца Google Play изисква SDK за реклами да деактивират персонализираните реклами, рекламирането въз основа на интереси и ремаркетинга.
- Дайте възможност на издателите да избират рекламни формати, които спазват [правилата на Google Play относно рекламите за семейства и осигуряването на приходи](#) и отговарят на изискването на [програмата „Одобreno от учители“](#).
- Уверете се, че когато за показване на реклами на деца се използва оферирание в реално време, файловете за създаване на реклама са прегледани и индикаторите за поверителност са стигнали до офериращите.

- Предоставете на Google достатъчно данни, като например тестово приложение и информацията, посочена във [формуляра за заявяване на интерес](#) по-долу, за да провери дали SDK за реклами отговаря на всички изисквания за самостоятелно сертифициране, и отговаряйте своевременно на всички последващи искания за информация, като например с изпращане на нови пуснати версии, за да се потвърди, че версията на SDK за реклами спазва всички изисквания за самостоятелно сертифициране, и с предоставяне на тестово приложение.
- [Сертифицирайте самостоятелно](#), че всички нови пуснати версии спазват актуалните програмни правила за програмистите в Google Play, включително изискванията в правилата за семейства.

Забележка: Самостоятелно сертифицираните SDK за реклами за семейства трябва да поддържат показване на реклами, спазващо всички приложими закони и разпоредби относно деца, които може да са в сила за съответните издатели.

Повече информация за поставянето на воден знак на рекламни послания и предоставянето на тестово приложение може да бъде намерена [тук](#).

Ето изискванията за посредничество за рекламни платформи, когато се показват реклами на деца:

- Използвайте само самостоятелно сертифицирани SDK за реклами за семейства или внедрете необходимите предпазни мерки, така че всички реклами, показвани от посредническите мрежи, да отговарят на тези изисквания.
- Подавайте на платформите за посредничество необходимата информация, с която да посочите класификацията на рекламното съдържание и всяко приложимо третиране като предназначено за деца.

[Тук](#) програмистите могат да намерят списък със самостоятелно сертифицираните SDK за реклами за семейства и да проверят кои конкретни версии на тези SDK са самостоятелно сертифицирани за използване в приложенията за семейства.

Освен това те имат възможност да споделят този [формуляр за заявяване на интерес](#) с доставчиците на SDK за реклами, които искат да се сертифицират самостоятелно.

Малка обява в магазина и популяризация

Популяризацията и видимостта на приложението ви се отразяват драстично върху качеството на магазина. Избягвайте малки обяви, съдържащи спам, популяризиране с ниско качество, както и опити за изкуствено повишаване на видимостта на приложението в Google Play.

Популяризация на приложения

Не допускаме приложения, които пряко или косвено участват във или се възползват от практики за популяризиране (като например реклами), които са подвеждащи или вредни за потребителите или екосистемата от програмисти. Практиките са подвеждащи или вредни, ако поведението или съдържанието им нарушават програмните ни правила за програмистите.

Ето няколко примера за често срещани нарушения:

- Използване на [подреждащи](#) реклами в уебсайтове, приложения или други собственоности, включително известия, които са подобни на системните известия и сигнали.
- Използване на реклами с [явен сексуален характер](#) за насочване на потребителите към малката обява в Google Play на приложението ви с цел изтегляне.

- Похвати за популяризиране или инсталиране, които пренасочват потребителя към Google Play или при които се изтеглят приложения без информираното му действие.
- Нежелано популяризиране посредством SMS услуги.
- Текст или изображение в името на приложението, иконата или името на програмиста, които указват ефективност или класиране в магазина, цена или промоционална информация или предполагат връзка със съществуващи програми в Google Play.

Ваша отговорност е да гарантирате, че всички рекламни мрежи, партньори или реклами, свързани с приложението ви, спазват тези правила.

Метаданни

Потребителите разчитат на описанията на приложението ви, за да разберат какви са функционалността и предназначението му. Не допускаме приложения с подвеждащи, неправилно форматираны, неописателни, неуместни, прекомерни или неподходящи метаданни, включително, без изброяването да е изчерпателно, в описанието на приложението, името на програмиста, заглавието, иконата, екранните снимки и изображенията за популяризиране. Програмистите трябва да предоставят ясно и добре написано описание за приложението си. Също така не разрешаваме в описанието да има анонимни потребителски мнения или такива без означение за авторство.

Името ви на програмист, заглавието и иконата на приложението ви са особено полезни за потребителите – така те намират приложението ви и научават повече за него. Не използвайте емоджи, емотикони или повтарящи се специални знаци в тези метаданни. Не използвайте САМО ГЛАВНИ БУКВИ, освен ако не са част от името на марката ви. Не се допускат подвеждащи символи в иконите на приложенията, като например точка, индикираща нови съобщения, когато няма такива, и символи за изтегляне/инсталиране, когато приложението не е свързано с изтегляне на съдържание. Заглавието на приложението ви трябва да е с дължина най-много 30 знака. Не използвайте текст или изображение в името на приложението, иконата или името на програмиста, които указват ефективност или класиране в магазина, цена или промоционална информация или предполагат връзка със съществуващи програми в Google Play.

В допълнение към посочените тук изисквания конкретни правила за програмистите в Google Play може да изискват да предоставите допълнителни метаданни.

Ето няколко примера за често срещани нарушения:

- ① Анонимни потребителски мнения или такива без означение за авторство.
- ② Сравняване на данните на приложения или търговски марки.
- ③ Блокове от думи и вертикални/хоризонтални списъци с думи.

- ① САМО ГЛАВНИ БУКВИ, въпреки че не са част от името на марката.
- ② Поредици от специални знаци, които не са свързани с приложението.
- ③ Използване на емоджи, емотикони (включително као моджи) и специални знаци.
- ④ Подвеждащи символи.
- ⑤ Подвеждащ текст.

- Изображения или текст, които споменават ефективността или класирането в магазина, като например „Приложение на годината“, „№1“, „Най-доброто в Google Play за 20XX“, „Популярно“, икони за отличия и др.

- Изображения или текст, които споменават цени и промоции, като например „10% отстъпка“, „Връщане на 50 щ.д.“, „Безплатно за ограничено време“ и гр.

- Изображения и текст, които споменават програми на Google Play, като например „Избор на редактора“, „Ново“ и гр.

Ето няколко примера за неподходящ текст, изображения или видеоклипове в малката ви обява:

- Изображения или видеоклипове със съдържание със сексуален характер. Избягвайте предизвикващи неприлични асоциации изображения, съдържащи гърди, задни части, гениталии или друг вид фетишизирани телесни части или съдържание, независимо дали е реално, или илюстративно.
- Използване на непристоен, вулгарен или друг език, който е неподходящ за широката аудитория в малката обява в магазина за приложението ви.

- Детайлно и ясно показано насилие в икони на приложението, изображения за популяризиране или видеоклипове.
- Показване на забранена употреба на наркотици. Дори съдържанието с образователен, документален, научен или художествен характер трябва да е подходящо за всички аудитории в малката обява в магазина.

Ето няколко най-добри практики:

- Открийте силните страни на приложението си. Споделете с потребителите интересни и възбудяващи факти за него. Погрижете се да разберат какво го отличава от останалите.
 - Уверете се, че името и описанието на приложението ви обрисуват точно функционалността му.
 - Избягвайте използването на повтарящи се или неуместни ключови думи или препратки.
 - Описанието на приложението ви трябва да е сбито и ясно. По-кратките описания обикновено се четат по-лесно, особено на устройства с по-малки екрани. Твърде големият обем, неправилното форматиране и прекалените подробности и повторения могат да доведат до нарушение на тези правила.
 - Не забравяйте, че малката ви обява трябва да е подходяща за широката аудитория. Не използвайте неуместни текст, изображения или видеоклипове в нея и спазвайте указанията по-горе.
-

Оценки от потребители, отзиви и инсталирания

Програмистите не трябва да опитват да манипулират разположението на приложенията в Google Play. Това включва, без изброяването да е изчерпателно, изкуствено повишаване на оценките или броя инсталирания на продуктите или подобряване на отзивите чрез незаконни средства, като например измамнически или получени срещу поощрение отзиви и оценки, или поощряване на потребителите да инсталират други приложения като основна функционалност на приложението.

Ето няколко примера за често срещани нарушения:

- Молите потребителите да оценят приложението ви и същевременно предлагате поощрение:

① Това известие предлага на потребителите отстъпка в замяна на висока оценка.

- Многократно изпращане на оценки, представени като такива от потребители, с цел да се повлияе върху разположението на приложението в Google Play.
- Изпращане или насърчаване на потребителите да изпращат отзиви с неподходящо съдържание, включително партньори, талони, кодове за игри, имейл адреси или връзки към уебсайтове или други приложения:

② Този отзив насърчава потребителите да популяризират приложението RescueRover, като им предлага талон.

Оценките и отзивите са показатели за качеството на приложенията. Потребителите разчитат те да са автентични и уместни. Ето няколко най-добри практики, когато отговаряте на отзиви от потребители:

- Съсредоточете отговора си върху проблемите, посочени в коментарите на потребителя, и не искайте по-висока оценка.
 - Включете препратки към полезни ресурси, като например адрес за поддръжка или страница с често задавани въпроси.
-

Класификации на съдържанието

Класификациите на съдържанието в Google Play се предоставят от [Международната коалиция за възрастово класифициране \(IARC\)](#) и имат за цел да помагат на програмистите да информират потребителите за подходяща за местните условия класификация. Регионалните органи на IARC поддържат указания, които се използват за определяне на нивото на зрелост на съдържанието в приложението. Не допускаме в Google Play приложения без класификация на съдържанието.

Начин на използване на класификацията на съдържанието

Класификацията на съдържанието се използва, за да информира потребителите – особено родителите – за потенциално непристойно съдържание в приложението. Тя също така помага за филтрирането или блокирането на съдържанието ви в определени територии или за конкретни потребители, когато това се изисква по закон, и определя дали приложението ви отговаря на условията за специални програми за програмисти.

Как се определя класификацията на съдържанието

За да получите класификация на съдържанието, трябва да попълните [съответния въпросник в Play Console](#), в който се пита за естеството на съдържанието на приложението ви. Въз основа на отговорите ви на приложението ви ще бъде присвоена класификация на съдържанието от няколко органа за целта. Подвеждащото представяне на съдържанието на приложението ви може да доведе до премахване или спиране. Затова е важно да давате точни отговори във въпросника за класификация на съдържанието.

За да не допуснете липса на класификация за приложението си, трябва да попълвате въпросника за класификация на съдържанието за всяко ново приложение, което изпращате в Play Console, както и за всички съществуващи приложения, активни в Google Play. Приложенията без класификация на съдържанието ще бъдат премахвани от Google Play Магазин.

Ако извършите промени в съдържанието или функциите на приложението си, които се отразяват върху отговорите ви на въпросника за класификация, трябва да изпратите нов такъв въпросник в Play Console.

Посетете [Помощния център](#), за да намерите повече информация за различните [органи за класификация](#) и за попълването на въпросника за класификация на съдържанието.

Обжалване на класификации

Ако не приемате класификацията, присвоена на приложението ви, можете да обжалвате директно пред органа за класификация IARC посредством връзката, посочена в имейла ви за сертификат.

Новини

Приложенията за новини са такива, които:

- декларират в Play Console, че са за новини;
- са включени в категорията „Новини и списания“ в Google Play Магазин и в името, иконата, името на програмиста или описанието им е посочено, че са за новини.

Примери за приложения в категорията „Новини и списания“, които отговарят на изискванията за приложения за новини:

- приложения, в чието описание е посочено, че са за новини, включително, без изброяването да е изчерпателно:
 - последни новини;
 - вестници;
 - извънредни новини;
 - местни новини;
 - ежедневни новини.
- приложения, които съдържат думата „новини“ в името/иконата си или в името на програмиста.

Ако обаче приложенията съдържат предимно съдържание, генерирано от потребителите (напр. приложения за социални медии), те не трябва да декларират, че са за новини, и не се считат за такива.

Приложенията за новини, които изискват от потребителя да купи членство, трябва да му предоставят визуализация на съдържанието в тях преди покупката.

Приложенията за новини трябва:

- да предоставят информация за собственика на приложението и източника на новинарските статии, включително, без изброяването да е изчерпателно, първоначалния издател или автор на всяка статия. Когато посочването на отделните автори на статиите не е обичайната практика, приложението за новини трябва да бъде първоначалният издател на статиите. Моля, обърнете внимание, че връзките към профили в социални медии не представляват достатъчна информация за автора или издателя.
- да имат специален уебсайт или страница в приложението, които са обозначени по ясен начин като съдържащи информация за връзка, могат да бъдат намерени лесно (напр. има връзка към тях в долната част на началната страница или в лентата за навигация на сайта) и предоставят валидна информация за връзка с издателя на новини, включваща имейл адрес или телефонен номер. Моля, обърнете внимание, че връзките към профили в социални медии не представляват достатъчна информация за контакт с издателя.

Приложенията за новини не трябва:

- да съдържат значителни правописни и/или граматични грешки;
- да съдържат само статично съдържание (напр. такова отпреди три месеца);
- да са такива, чиято основна цел е маркетинг чрез партньорски програми или приходи от реклами.

Моля, обърнете внимание, че приложенията за новини *може* да използват реклами и други форми на маркетинг, стига основната им цел да не е да продават продукти и услуги или да генерират приходи от реклами.

В приложенията за новини, които са агрегатори на съдържание от различни публикуващи източници, трябва да има прозрачност по отношение на публикуващия източник на съдържанието в тях и всеки източник трябва да спазва изискванията на правилата на Google Новини.

Моля, [прегледайте тази статия](#) , за да разберете как най-добре да предоставите необходимата информация.

Спам, функционалност и практическа работа на потребителите

Приложенията трябва да осигуряват на потребителите поне основни и подходящи функционалност и съдържание с цел ангажираща практическа работа. Приложения, които претърпяват сридове, демонстрират поведение, което не съответства на функционалната практическа работа, или служат само за да разпространяват спам до потребителите или в Google Play, не са смислено допълнение към каталога.

Спам

Не допускаме приложения, които разпространяват спам до потребителите или злоупотребяват с Google Play, например изпращат нежелани съобщения, копират други приложения или са с ниско качество.

Неупълномощено изпращане на съобщения

Не допускаме приложения, които изпращат имейли, SMS или други съобщения от името на потребителя, без да му предоставят възможност да потвърди съдържанието и получателите, за които е предназначено.

Ето пример за често срещано нарушение:

- Когато потребителят натисне бутона за споделяне, приложението изпраща съобщения от негово име, без да му предоставя възможност да потвърди съдържанието и получателите, за които е предназначено:

Непозволено използване на изгледи в мрежата и пренасочване към партньорско съдържание

Не допускаме приложения, чиято основна цел е да насочват трафик към партньорски уебсайтове или да предоставят изглед в мрежата на даден сайт без разрешение от собственика или администратора му.

Ето няколко примера за често срещани нарушения:

- Приложение, чиято основна цел е да препраща трафик към даден уебсайт, за да получи признание за регистрации на потребители или покупки в него.
- Приложения, чиято основна цел е да предоставят изглед в мрежата на даден уебсайт, без да имат разрешение за това:

① Това приложение се нарича Ted's Shopping Deals, но предоставя само изглед в мрежата на Google Пазаруване.

Повтарящо се съдържание

Не допускаме приложения, които не предлагат нищо по-различно от вече съществуващите в Google Play. Приложенията трябва да предоставят стойност на потребителите чрез създаване на уникални услуги и съдържание.

Ето няколко примера за често срещани нарушения:

- Копиране на съдържание от други приложения без добавяне на оригинално съдържание или стойност.
- Създаване на няколко приложения с много сходни съдържание и практическа работа на потребителите. Ако тези приложения са малки по обем, програмистите трябва да обмислят възможността да създадат едно приложение, включващо цялото съдържание.

Функционалност, съдържание и практическа работа на потребителите

Приложенията трябва да осигуряват стабилна, полезна и ангажираща практическа работа. Приложенията, които претърпяват сридове, не осигуряват поне основна и подходяща полезност като мобилни приложения, не предлагат интересно съдържание или

демонстрират поведение, което не съответства на функционалната и ангажираща практическа работа, не се допускат в Google Play.

Ограничена функционалност и съдържание

Не допускаме приложения, които имат само ограничена функционалност и съдържание.

Ето пример за често срещано нарушение:

- Приложения, които са статични и без конкретни за тях функции, като например приложения само с текст или такива за PDF файлове.
- Приложения, в които има много малко съдържание и които не предоставят ангажираща практическа работа на потребителите, като например приложения с един тапет.
- Приложения, които са създадени да не вършат нищо или нямат никаква функция.

Повредена функционалност

Не допускаме приложения, които претърпяват сридове, затварят се принудително, блокират или по друг начин функционират ненормално.

Ето няколко примера за често срещани нарушения:

- Приложения, които **не се инсталират**.
-

Приложения, които се инсталират, но **не се зареждат**.

•

Приложения, които се зареждат, но **не реагират** .

Други програми

Приложенията, предназначени за други типове работа с Android и разпространявани чрез Google Play, трябва да спазват правилата за съдържанието, изложени в други части от този Център за правила, а освен това за тях може да важат изисквания, свързани с правилата на конкретна програма. Разгледайте списъка по-долу и вижте дали някое от тези правила се отнася за приложението ви.

Мигновени приложения за Android

Целта ни е с мигновените приложения за Android да осигурим на потребителите приятна и безпроблемна работа, като същевременно спазваме най-високите стандарти за сигурност и поверителност. Правилата ни са предназначени да подкрепят тази цел.

Програмистите, които разпространяват мигновени приложения за Android посредством Google Play, трябва да спазват следните правила в допълнение към останалите [програмни правила за програмистите в Google Play](#).

Самоличност

При мигновените приложения с функция за влизане в профил програмистите трябва да внедрят [Smart Lock за пароли](#) .

Поддръжка на връзки

Програмистите на мигновени приложения за Android трябва пълноценно да поддържат връзки за други приложения. Ако инсталираните или мигновените приложения на програмиста съдържат връзки, които потенциално може да водят към мигновено приложение, програмистът трябва да насочва потребителите към съответното мигновено приложение, вместо връзките да стигат например до [WebView](#) .

Технически спецификации

Програмистите трябва да спазват предоставените от Google изисквания и технически спецификации (които може от време на време да бъдат променяни) за мигновените приложения за Android, включително посочените в [обществената ни документация](#).

Предлагане на инсталиране на приложение

Мигновеното приложение може да предлага на потребителя приложението, което се инсталира, но това не бива да е основната му цел. При предлагане на инсталиране програмистите трябва да спазват следното:

- Да използват [иконата за изтегляне на приложение съгласно Material Design](#) и текста „инсталиране“ за бутона за инсталиране.
- Мигновеното им приложение не бива да съдържа повече от 2 – 3 неявни подкани за инсталиране.
- Не бива да използват банер или друга техника, подобна на реклама, за да показват на потребителите подкана за инсталиране.

Можете да намерите още указания за практическата работа на потребителите и подробности за мигновените приложения на страницата с [най-добри практики за практическа работа на потребителите](#).

Промяна на състоянието на устройството

Мигновените приложения не бива да правят в устройството на потребителя промени, които се запазват след края на сесията на съответното приложение. Например не може да променят тапета на потребителя или да създават приспособление на началния екран.

Видимост на приложението

Програмистите трябва да се погрижат мигновените приложения да са видими за потребителите, така че те винаги да са наясно, че на устройствата им се изпълняват въпросните приложения.

Идентификатори на устройството

На мигновените приложения е забранен достъп до идентификатори на устройството, за които са изпълнени едновременно следните условия: (1) запазват се и след завършването на изпълнението на мигновеното приложение и (2) не могат да се задават повторно от потребителя. Примерите за това включват следното, като списъкът не е изчерпателен:

- сериен номер на компилацията;
- MAC адреси на чипове за мрежова връзка;
- IMEI, IMSI.

Мигновените приложения може да получат достъп до телефонния номер, ако това се извърши след разрешение по време на изпълнение. Програмистът не бива да опитва да идентифицира потребителя чрез тези идентификатори или други средства.

Трафик в мрежата

Трафикът в мрежата от мигновеното приложение трябва да бъде шифрован с протокол с TLS, като например HTTPS.

Правила на Android за емоджи

Правилата ни относно емоджи са създадени с цел популяризирането на приобщаваща и последователна практическа работа. За да постигнем това, всички приложения трябва да поддържат най-новата версия на [емоджи с уникод](#) , когато работят на устройства с Android 12 или по-нови версии.

Приложенията, които използват стандартните емоджи за Android без персонализирани решения за внедряване, вече използват най-новата версия на емоджи с уникод на устройства с Android 12 или по-нови версии.

Приложенията с персонализирани решения за внедряване на емоджи, включително предоставените чрез библиотеки на трети страни, трябва да поддържат изцяло най-новата версия на уникод на устройства с Android 12 и по-нови версии в рамките на 4 месеца след публикуването на новите емоджи с уникод.

Разгледайте това [ръководство](#) , за да научите как да поддържате съвременни емоджи.

Семейства

Google Play предлага на програмистите платформа с богати възможности за представяне на висококачествено и подходящо за съответните възрасти съдържание за цялото семейство. Преди да изпратите дадено приложение в програмата „Приложения за семейството“ или такова, което е предназначено за деца, в Google Play Магазин, трябва да се уверите, че то е подходящо за деца и че спазва всички приложими закони.

[Научете за процеса за семейства и прегледайте интерактивния контролен списък в Академията за създатели на приложения.](#)

Правила на Google Play за семейства

Технологиите все повече се използват, за да обогатяват живота на семействата, и родителите търсят безопасно и висококачествено съдържание, което да споделят с децата си. Възможно е приложенията ви да са предназначени специално за деца или някое от тях може да привлече вниманието им. Google Play иска да ви помогне да гарантирате, че приложението ви е безопасно за всички потребители, включително за семейства.

Думата „деца“ може да означава различни неща в различни локали и в различен контекст. Важно е да се консултирате с правен експерт, за да определите какви задължения и/или възрастови ограничения може да са в сила за приложението ви. Вие знаете най-добре как работи то, така че разчитаме на вас да ни помогнете приложенията в Google Play да бъдат безопасни за семейства.

За всички приложения, които спазват правилата на Google Play за семейства, може да се заяви оценяване за [програмата „Одобreno от учители“](#), но не можем да гарантираме, че приложението ви ще бъде включено в нея.

Изисквания на Play Console

Целева аудитория и съдържание

Преди да публикувате приложението си, трябва да посочите целевата му аудитория в секцията [Целева аудитория и съдържание](#) в Google Play Console, като изберете от предоставения списък с възрастови групи. Независимо от това, какво посочите в Google Play Console, ако решите да включите в приложението си изображения и терминология, за които може да се сметне, че са насочени към деца, това може да повлияе на оценката на Google Play за заявената от вас целева аудитория. Google Play си запазва правото да извърши собствен преглед на предоставената от вас информация за приложението, за да определи дали целевата аудитория, която сте посочили, е точна.

Трябва да изберете повече от една възрастова група за целевата аудитория на приложението си само ако сте го създали специално за потребителите в избраните възрастови групи и сте сигурни, че то е подходящо за тях. Например за приложенията, предназначени за бебета и за деца в предучилищна възраст, трябва да изберете само „До 5 год. вкл.“ за целева възрастова група. Ако приложението ви е създадено за конкретен образователен етап, посочете най-подходящата възрастова група. Трябва да изберете възрастови групи, които включват както възрастни, така и деца само ако приложението ви наистина е предназначено за всички възрасти.

Актуализации в секцията „Целева аудитория и съдържание“

Винаги можете да актуализирате информацията за приложението си в секцията „Целева аудитория и съдържание“ в Google Play Console. Необходима е [актуализация на приложението](#), преди съответната промяна да бъде отразена в Google Play Магазин. Всички промени, които направите в тази секция на Google Play Console, обаче може да преминат преглед за спазване на правилата още преди изпращането на актуализация.

Ако промените целевата възрастова група за приложението си или започнете да използвате реклами или да предлагате покупки в него, настоятелно ви препоръчваме да уведомите съществуващите потребители посредством секцията „Новите неща“ на страницата на малката обява в магазина или чрез известия в приложението.

Подвеждащо представяне в Play Console

Подвеждащото представяне на информация за приложението ви в Play Console, включително в секцията „Целева аудитория и съдържание“, може да доведе до премахване или спиране на приложението. Затова е важно да предоставяте точна информация.

Изисквания за съдържанието за семейства

Ако децата са сред целевите аудитории за приложението ви, трябва да спазвате следните изисквания. Неспазването им може да доведе до неговото премахване или спиране.

- 1. Съдържание на приложението:** Съдържанието, което е достъпно за деца, трябва да е подходящо за тях. Ако в приложението ви има съдържание, което не е подходящо навсякъде по света, но се смята, че е подходящо за непълнолетни потребители в конкретен регион, приложението може да е налице в този регион ([ограничени региони](#)), но ще остане недостъпно в другите.
- 2. Функции на приложението:** Приложението ви не трябва да предоставя само WebView на гаден уебсайт или да има за основна цел да насочва трафик към партньорски уебсайт, без да има разрешение от съответния собственик или администратор.
- 3. Отговори в Play Console:** Трябва да отговорите точно на въпросите в Play Console относно приложението ви и да актуализирате отговорите си, така че да отразяват точно всички промени в него. Това включва, без изброяването да е изчерпателно, предоставяне на точни отговори за приложението ви в секцията „Целева аудитория и съдържание“, секцията за безопасност на данните и въпросника на IARC за класификация на съдържанието.
- 4. Практики за данни:** Трябва да разкриете как приложението ви събира [лична и поверителна информация](#) от деца, включително чрез извикванията или използваните в него API и SDK. Поверителната информация от деца включва, без изброяването да е изчерпателно, удостоверителни данни, информация от камерата и микрофона, данни на устройството, идентификатор за Android и данни за използването на реклами. Трябва също да гарантирате, че приложението ви спазва голупосочените [практики за данни](#):
 - Приложенията, предназначени само за деца, не трябва да предават следните данни: идентификатор за рекламиране за Android, сериен номер на SIM картата, сериен номер на компилацията, BSSID, MAC адрес, SSID, IMEI и/или IMSI номер.

- Приложенията, които са изцяло насочени към деца, не трябва да искат разрешението AD_ID, когато са насочени към API ниво 33 или по-високо на Android.
 - Приложенията, които са насочени към аудитория от деца и по-възрастни потребители, не трябва да предават следните данни от деца или потребители с неизвестна възраст: AAID, сериен номер на SIM картата, сериен номер на компилацията, BSSID, MAC адрес, SSID, IMEI и/или IMSI номер.
 - Телефонният номер на устройството не трябва да бъде изискван от TelephonyManager в API на Android.
 - Приложенията, предназначени само за деца, не може да заявяват разрешение за достъп до местоположението, нито да събират, използват и предават [точното местоположение](#).
 - Приложенията трябва да използват [инструмента за управление на придружаващи устройства \(CDM\)](#) , когато искат достъп до Bluetooth, освен ако не са насочени само към версии на мобилната операционна система, които не са съвместими със CDM.
5. **API и SDK:** Всички API и SDK трябва да са внедрени правилно в приложението ви.
- Приложенията, предназначени само за деца, не трябва да съдържат API и SDK, които не са одобрени за използване в насочени основно към деца услуги.
 - Например услуга за API, използваща технологията OAuth за удостоверяване и упълномощаване, в чиито общи условия е посочено, че не е одобрена за използване в услуги, насочени към деца.
 - В приложенията, предназначени както за деца, така и за възрастни, не трябва да се внедряват API или SDK, които не са одобрени за използване в насочени към деца услуги, освен ако не се използват след [неутрално отсяване по възраст](#) или не са внедрени по начин, който не води до събирането на данни от деца. Приложенията, които са насочени към аудитория от деца и по-възрастни потребители, не трябва да изискват от потребителите да осъществяват достъп до съдържанието чрез API и SDK, които не са одобрени за използване в насочени към деца услуги.
6. **Обогатена реалност (AR):** Ако приложението ви използва обогатена реалност, трябва да включите предупреждение за безопасност, което се показва веднага след стартирането на секцията за AR. Предупреждението трябва да съдържа следните неща:
- подходящо съобщение за важността на родителския контрол;
 - напомняне за физическите опасности в реалния свят (например да се има предвид заобикалящата среда).
 - Приложението ви не трябва да изисква използването на устройство, което е препоръчително да не се ползва от деца (например Daydream, Oculus).
7. **Социални приложения и функции:** Ако приложението ви позволява на потребителите да споделят или обменят информация, трябва точно да разкриете тези функции във [Въпросника за класификация на съдържанието](#) в Play Console.
- Социални приложения: Социалното приложение е такова приложение, чието основно предназначение е да даде възможност на потребителите да споделят съдържание в свободна форма или да общуват с големи групи хора. Всички социални приложения, в чиято целева аудитория са включени деца, трябва да извеждат напомняне в приложението относно безопасността онлайн и реалния риск при общуването онлайн, преди да разрешат на децата да споделят мултимедия или информация в свободна форма. Също така трябва да изискват действие от страна на възрастен, преди да разрешите на децата да споделят лична информация.
 - Социални функции: Социалната функция е всяка допълнителна функционалност на приложението, която позволява на потребителите да споделят съдържание в свободна форма или да общуват с големи групи хора. Всяко приложение, в чиято целева аудитория са включени деца и което има социални функции, трябва да извежда напомняне в приложението относно безопасността онлайн и реалния риск при общуването онлайн,

преди да разреши на децата да споделят мултимедия или информация в свободна форма. Също така трябва да предоставите начин, чрез който възрастните да могат да управляват социалните функции, достъпни за децата, включително, но не само, да активират/деактивират дадена социална функция или да изберат други нива на функционалност. И накрая, трябва да изисквате действие от страна на възрастен преди активирането на функции, които позволяват на децата да споделят лична информация.

- Действието от страна на възрастен означава механизъм за потвърждаване, че въпросният потребител не е дете, който освен това не насърчава децата да фалшифицират възрастта си, за да получат достъп до областите в приложението, създадени за възрастни (напр. свързани с възрастен ПИН код, парола, дата на раждане, потвърждаване на имейл, документ за самоличност със снимка, кредитна карта или социалноосигурителен номер).
- Социалните приложения, чието основно предназначение са разговори с непознати, не трябва да са насочени към деца. Примерите включват: приложения от типа на Chat Roulette, приложения за запознанства, фокусиращи се върху деца отворени стаи за чат и др.

8. **Спазване на законите:** Приложението ви (включително всички API или SDK, които то извиква или използва) трябва да спазва [американския Закон за защита на личната неприкосновеност на децата онлайн \(COPPA\)](#) , [Общия регламент на ЕС относно защитата на данните \(ОРЗД\)](#) и всички други приложими закони и разпоредби.

Ето няколко примера за често срещани нарушения:

- Приложения, в чиято малка обява в магазина се популяризира игра за деца, но съдържанието им е подходящо само за възрастни.
- Приложения, които внедряват API с общи условия, забраняващи използването им в приложения, предназначени за деца.
- Приложения, които представят в привлекателна светлина употребата на алкохол, тютюневи изделия или контролирани вещества.
- Приложения, които включват истински хазарт или наподобяване на хазартни игри.
- Приложения със съдържание, което е шокиращо или включва насилие или кръвопролитие и не е подходящо за деца.
- Приложения, предлагащи услуги за запознанства или сексуални или брачни съвети.
- Приложения с връзки към уебсайтове, представящи съдържание, което нарушава [програмните правила за програмистите](#) в Google Play.
- Приложения, в които на деца се показват реклами за пълнолетни (напр. съдържание с насилие, сексуално съдържание и съдържание, свързано с хазарт).

Реклами и осигуряване на приходи

Ако си осигурявате приходи от приложение, насочено към деца в Google Play, е важно то да следва изискванията на следните правила относно рекламите за семейства и осигуряването на приходи.

Правилата по-долу се отнасят за всички случаи на осигуряване на приходи и рекламиране в приложението ви, включително реклами, крос-медийно популяризиране (на вашите приложения и тези на трети страни), оферти за покупки в приложения или всяко друго рекламно съдържание (например платено продуктово позициониране). Всички случаи на осигуряване на приходи и рекламиране в тези приложения трябва да спазват приложимите закони и разпоредби (включително всички съответни правила за саморегулиране и отраслови стандарти).

Google Play си запазва правото да отхвърля, премахва или спира приложения заради прекалено агресивна рекламна стратегия.

Изисквания за рекламите

Ако приложението ви показва реклами на деца или на потребители с неизвестна възраст, трябва:

- да използвате само [самостоятелно сертифицирани SDK за реклами за семейства в Google Play](#) за показване на реклами на тези потребители;
- показваните реклами да не включват рекламиране въз основа на интереси (реклами, насочени към отделни потребители с определени характеристики въз основа на поведението им при сърфиране онлайн) или ремаркетинг (реклами, насочени към отделни потребители въз основа на предишно взаимодействие с дадено приложение или уебсайт);
- съдържанието на показваните реклами да е подходящо за деца;
- показваните реклами да отговарят на изискванията за рекламния формат за семейства;
- да спазвате приложимите правни разпоредби и отраслови стандарти, свързани с рекламирането пред деца.

Изисквания за рекламния формат

Осигуряването на приходи и рекламите в приложението ви не трябва да са с измамно съдържание, нито да са с такъв дизайн, че да водят до случайни кликания от потребители деца.

Ако приложението ви е изцяло насочено към деца, следните неща са забранени. В случай че целевата аудитория на приложението ви е от деца и по-възрастни хора, долуизброените неща са забранени, когато се показват реклами на деца и потребители с неизвестна възраст:

- наtrapчиво осигуряване на приходи и реклами, включително такива, които заемат целия екран или възпрепятстват нормалното използване и не предоставят ясен начин за отхвърлянето си (например [реклами на цял екран](#));
- осигуряване на приходи и реклами, които възпрепятстват обичайното използване на приложението или начина на игра, включително реклами с поощрение или избор, които не могат да бъдат затворени след 5 секунди;
- осигуряването на приходи и рекламите, които не възпрепятстват обичайното използване на приложението или начина на игра, може да се задържат повече от 5 секунди (например видеосъдържание с интегрирани реклами);
- осигуряване на приходи и реклами посредством заставки, които се показват веднага след стартирането на приложението;
- разполагане на няколко реклами на една страница (например не се разрешават банерни реклами, които показват няколко предложения в едно разположение или съдържат повече от един банер или видеореклами);
- осигуряване на приходи и реклами, които не се отличават ясно от съдържанието на приложението, като например offerwall и други грабващи вниманието реклами;
- използване на шокиращи или емоционално манипулативни тактики за насърчаване на гледането на реклами или покупки в приложението;
- подвеждащи реклами, които принуждават потребителя да кликне върху тях, като натисне бутон за отхвърляне, който задейства друга реклама, или като се показват внезапно в части от приложението, където потребителят обикновено докосва, за да използва друга функция;
- липсата на разграничение между използването на виртуални монети и истински пари за извършването на покупки в приложението.

Ето няколко примера за често срещани нарушения:

- Осигуряване на приходи и реклами, които се отдалечават от пръста на потребителя при опит да бъдат затворени.

- Осигуряване на приходи и реклами, които не дават на потребителя възможност да излезе от офертата след 5 секунди, както е показано в примера по-долу:

- Осигуряване на приходи и реклами, които заемат по-голямата част от екрана на устройството, без да предлагат на потребителя ясен начин да ги отхвърли, както е показано в примера по-долу:

- Банерни реклами с няколко оферти, както е показано в примера по-долу:

- Осигуряване на приходи и реклами, които потребителят може да сбърка със съдържание на приложението, както е показано в примера по-долу:

- Бутони, реклами или други начини за осигуряване на приходи, които популяризират другите ви малки обяви в Google Play Магазин, но са неразличими от съдържанието на приложението, както е показано в примера по-долу:

Ето няколко примера за неподходящо рекламно съдържание, което не трябва да се показва на деца.

- **Неподходящо мултимедийно съдържание:** Реклами за телевизионни предавания, филми, музикални албуми или друго мултимедийно съдържание, което не е подходящо за деца.
- **Неподходящи видеоигри и софтуер за изтегляне:** Реклами за софтуер за изтегляне и електронни видеоигри, които не са подходящи за деца.
- **Контролирани или вредни вещества:** Реклами за алкохол, тютюневи изделия, контролирани или други опасни вещества.
- **Хазарт:** Реклами за популяризиране на хазартни симулатори, състезания или тотализатори дори ако участието е безплатно.
- **Съдържание за възрастни или такова, предизвикващо сексуални асоциации:** Реклами със сексуално съдържание или с такова, което предизвиква сексуални асоциации или е предназначено за възрастни.
- **Запознанства или връзки:** Реклами за сайтове за запознанства или връзки между възрастни.
- **Съдържание с насилие:** Реклами със съдържание с насилие и шокиращи подробности, което не е подходящо за деца.

SDK за реклами

Ако показвате реклами в приложението си и целевата му аудитория включва единствено деца, трябва да използвате само версиите на [самостоятелно сертифицирани SDK за реклами за семейства](#) . Ако приложението е насочено както към деца, така и към по-възрастни потребители, трябва да въведете мерки за отсяване по възраст, като например [неутрално отсяване по възраст](#) , и да се погрижите рекламите за деца да се показват само чрез версиите на самостоятелно сертифицирани SDK за реклами в Google Play.

Направете справка със страницата с правилата на [програмата за самостоятелно сертифицирани SDK за реклами за семейства](#) , за да видите повече информация за тези изисквания. [Тук](#) можете да видите актуалния списък с версиите на самостоятелно сертифицирани SDK за реклами за семейства.

Ако използвате AdMob, направете справка с [Помощния център на програмата](#) за повече информация относно продуктите в нея.

Ваше задължение е да се погрижите приложението ви да отговаря на всички изисквания относно рекламите, покупките в приложения и рекламното съдържание. Свържете се с доставчиците на използваните от вас SDK за реклами, за да научите повече за съответните правила за съдържанието и рекламни практики.

Правила за самостоятелно сертифицираните SDK за реклами за семейства

Google Play полага всички усилия да създаде безопасна практическа работа за деца и семейства. Затова е важно да гарантираме, че децата виждат само реклами, които са подходящи за възрастта им, и че данните им се обработват според правилата. За да се постигне тази цел, изискваме SDK за реклами и платформите за посредничество да сертифицират самостоятелно, че са подходящи за деца и че спазват [програмните правила за програмистите в Google Play](#) и [правилата на Google Play за семейства](#) , включително изискванията относно [програмата за самостоятелно сертифицирани SDK за реклами за семейства](#) .

Програмата на Google Play за самостоятелно сертифицирани SDK за реклами за семейства е важен инструмент, с който програмистите идентифицират кои SDK за реклами или платформи за посредничество са сертифицирали самостоятелно, че са подходящи за използване в приложения, създадени специално за деца.

Подвеждащото представяне на информация за вашия SDK, включително във [формуляра ви за заявяване на интерес](#) , може да доведе до премахване вашия SDK от програмата за самостоятелно сертифицирани SDK за реклами за семейства или до неговото спиране. Затова е важно да предоставяте точна информация.

Изисквания, свързани с правилата

Ако вашият SDK или платформата ви за посредничество обслужват приложения, които са част от програмата „За семейството“ на Google Play, трябва да спазвате всички програмни правила за програмистите в Google Play, включително изискванията по-долу. Неспазването им може да доведе до премахване или спиране от програмата за самостоятелно сертифицирани SDK за реклами за семейства.

Ваше задължение е да се уверите, че вашият SDK или платформата ви за посредничество спазват правилата. Затова прегледайте [програмните правила за програмистите в Google Play](#), [правилата на Google Play за семейства](#) и [изискванията за програмата за самостоятелно сертифицирани SDK за реклами за семейства](#).

1. **Рекламно съдържание:** Рекламното съдържание, което е достъпно за деца, трябва да е подходящо за тях.

- Трябва (i) да дефинирате нежеланото рекламno съдържание и поведение и (ii) да ги забраните в общите условия или правилата си. Дефинициите трябва да спазват

[програмните правила за програмистите в Google Play.](#)

- Също така трябва да създадете метод за класифициране на рекламните си послания според възрастовите групи, за които са подходящи. Групите трябва да включват поне „За всички възрасти“ и „За пълнолетни“. Методологията за класифициране трябва да съответства на тази, която Google предоставя на SDK, след като програмистите са попълнили [формуляра за заявяване на интерес](#).
 - Трябва да се уверите, че когато за показване на реклами на деца се използва оферирание в реално време, файловете за създаване на реклама са прегледани и спазват горепосочените изисквания.
 - Освен това трябва да разполагате с [механизъм за визуално идентифициране на рекламните послания](#), за да проверявате дали са от съответните рекламни места (например чрез поставяне на воден знак на рекламните послания – това може да бъде логото на дружеството ви или друг визуален елемент с подобна функция).
2. **Рекламен формат:** Трябва да се уверите, че всички реклами, които се показват на непълнолетни потребители, отговарят на изискванията за рекламния формат за семейства. Също така трябва да предоставите възможност на програмистите да избират измежду рекламни формати, които спазват [правилата на Google Play за семейства](#).
- Рекламите не трябва да са с измамно съдържание, нито да са с такъв дизайн, че да водят до случайни кликания от деца. Не се допускат подвеждащи реклами, които принуждават потребителя да кликне върху тях, като натисне бутон за отхвърляне, който задейства друга реклама, или като се показват внезапно в части от приложението, където потребителят обикновено докосва, за да използва друга функция.
 - Не се допускат натрапчиви реклами, включително такива, които заемат целия екран или възпрепятстват нормалното използване и не предоставят ясен начин за отхвърлянето си (например [реклами на цял екран](#)).
 - Рекламите, които възпрепятстват нормалното използване на приложението или начина на игра, включително реклами с поощрение или избор, трябва да могат да бъдат затворени след 5 секунди.
 - Не се допуска разполагането на няколко реклами на една страница. Не се допускат например банерни реклами, които показват няколко предложения в едно разположение или съдържат повече от един банер или видеореклама.
 - Рекламите трябва да са ясно различни от съдържанието на приложението. Не се допускат съобщения от типа Offerwall и грабващи вниманието реклами, които не са ясно различни за непълнолетните потребители.
 - Рекламите не трябва да използват шокиращи или емоционално манипулативни тактики с цел насърчаване на гледането.
3. **IBA/ремаркетинг:** Трябва да се уверите, че рекламите, които се показват на непълнолетни потребители, не включват рекламиране въз основа на интереси (реклами, насочени към отделни потребители с определени характеристики въз основа на поведението им при сърфиране онлайн) или ремаркетинг (реклами, насочени към отделни потребители въз основа на предишно взаимодействие с дадено приложение или уебсайт).
4. **Практики за данни:** В качеството си на доставчик на SDK трябва да осигурите прозрачност относно начина, по който обработвате потребителски данни (например информация, събирана от или за потребителя, включително данни за устройството). Това означава да разкривате достъпа, събирането, използването и споделянето на данните от страна на своя SDK и да ги използвате само за оповестените цели. Тези изисквания на Google Play допълват изискванията на приложимите закони за поверителност и защита на данните. Трябва да разкриете как събирате [лична и поверителна информация](#) от деца, включително, без изброяването да е изчерпателно, удостоверителни данни, информация от камерата и микрофона, данни на устройството, идентификатор за Android и данни за използването на реклами.

- Трябва да разрешите на програмистите да поискат (въз основа на заявка или за отделно приложение) показваните реклами да се третират като предназначени за деца. Третирането им по този начин трябва да спазва приложимите закони и разпоредби, като например [Закон за защита на личната неприкосновеност на децата онлайн \(COPPA\) в САЩ](#) и [Общия регламент относно защитата на данните \(ОРЗД\) в ЕС](#).
 - Като част от третирането на рекламите като предназначени за деца Google Play изисква SDK за реклами да деактивират персонализираните реклами, рекламирането въз основа на интереси и ремаркетинга.
 - Трябва да се уверите, че когато за показване на реклами на деца се използва оферирание в реално време, индикаторите за поверителност са стигнали до офериращите.
 - Не трябва да предавате следните данни от деца или потребители с неизвестна възраст: AAID, сериен номер на SIM картата, сериен номер на компилацията, BSSID, MAC, SSID, IMEI и/или IMSI номер.
5. **Платформи за посредничество:** Когато се показват реклами на деца, трябва да изпълните следните изисквания:
- Използвайте само самостоятелно сертифицирани SDK за реклами за семейства или внедрете необходимите предпазни мерки, така че всички реклами, показвани от посредническите мрежи, да отговарят на тези изисквания.
 - Подавайте на платформите за посредничество необходимата информация, с която да посочите класификацията на рекламното съдържание и всяко приложимо третиране като предназначено за деца.
6. **Самостоятелно сертифициране и спазване на изискванията:** Трябва да предоставите на Google достатъчно данни, като например информацията, посочена във [формуляра за заявяване на интерес](#), за да провери дали SDK за реклами отговаря на всички изисквания за самостоятелно сертифициране, включително, без изброяването да е изчерпателно:
- предоставянето на версия на английски език на документацията (общите условия, декларацията за поверителност и ръководството за интегриране за издатели) на вашия SDK или платформата ви за посредничество.
 - изпращането на [примерно тестово приложение](#), използващо най-новата версия на съответния SDK за реклами, която спазва правилата. Примерното тестово приложение трябва да е изцяло компилиран и изпълним APK файл, който използва всички функции на съответния SDK. Изисквания за тестовото приложение:
 - Трябва да се изпрати като изцяло компилиран изпълним APK файл за Android, предназначен за работа с телефон.
 - Трябва да използва най-новата публикувана версия на SDK за реклами или версия, която предстои да бъде публикувана и спазва правилата на Google Play.
 - Трябва да използва всички функции на вашия SDK за реклами, включително да може да извиква съответния SDK, за да извлича и показва реклами.
 - Трябва да има пълен достъп до всички активни/действащи рекламни места от мрежата чрез рекламните послания, заявени от тестовото приложение.
 - Не трябва да е ограничено до конкретна геолокация.
 - Ако рекламните ви места са предназначени за смесена аудитория, тестовото приложение трябва да е в състояние да разграничава между заявките за рекламни послания от пълния набор места и такива от набора, подходящ за деца или всички възрастови групи.
 - Не трябва да бъде ограничено до конкретни реклами в рекламните места, освен ако не се контролира от механизъм за неутрално отсяване по възраст.
7. Трябва да отговаряте своевременно на всички последващи искания за информация и [самостоятелно да сертифицирате](#), че всички нови версии спазват най-новите програмни правила за програмистите в Google Play, включително изискванията на правилата за семейства.

8. **Спазване на законите:** Самостоятелно сертифицираните SDK за реклами за семейства трябва да поддържат показване на реклами, спазващо всички приложими закони и разпоредби относно деца, които може да са в сила за съответните издатели.

- Трябва да се уверите, че вашият SDK или платформата ви за посредничество спазват [Закон за защита на личната неприкосновеност на децата онлайн \(COPPA\) в САЩ](#) , [Общия регламент относно защитата на данните \(ОРЗД\) в ЕС](#) и всички други приложими закони и разпоредби.

Забележка: Думата „деца“ може да означава различни неща в различни локали и в различен контекст. Важно е да се консултирате с правен експерт, за да определите какви задължения и/или възрастови ограничения може да са в сила за приложението ви. Вие знаете най-добре как работи то, така че разчитаме на вас да ни помогнете приложенията в Google Play да бъдат безопасни за семейства.

За повече информация за съответните изисквания вижте страницата на [програмата за самостоятелно сертифицирани SDK за реклами за семейства](#).

Налагане на мерки

Винаги е по-добре да избягваме нарушенията на правилата, отколкото да се справяме с тях след възникването им. Поели сме ангажимент обаче в случай на нарушение да помогнем на програмистите да разберат как да приведат приложенията си в съответствие с правилата. Моля, уведомете ни, ако [забележите нарушения](#) или имате въпроси относно [справянето с тях](#) .

Обхват на правилата

Правилата ни са в сила за всяко съдържание, което се показва в приложението ви или към което има връзки в него. Това включва всички изведжани в приложението реклами и всяко генерирано от потребителите съдържание, което се хоства от него или към което то води. Правилата обхващат и съдържанието в профила ви на програмист, което се показва обществено в Google Play, включително името ви на програмист и целевата страница на посочения от вас уебсайт на програмиста.

Не допускаме приложения, които дават възможност на потребителите да инсталират други приложения на устройствата си. Приложенията, които осигуряват достъп на други приложения, игри или софтуер без инсталиране, включително функции и възможности, предоставяни от трети страни, трябва да обезпечат спазването на всички [правила на Google Play](#) за цялото съдържание, до което дават достъп. Също така е възможно да бъдат преглеждани допълнително за съответствие с правилата.

Дефинираните термини, използвани в тези правила, имат същото значение като в [Споразумението с програмистите относно разпространението](#). Освен че трябва да спазва настоящите правила и това споразумение, съдържанието на приложението ви трябва да бъде класифицирано съгласно съответните ни [указания](#).

Не допускаме приложения или съдържание, които подкопават доверието на потребителите в екосистемата на Google Play. Когато преценяваме дали да включим или премахнем дадено приложение от Google Play, вземаме предвид редица фактори, включително, без изброяването да е изчерпателно, модел на опасно поведение или голям риск от злоупотреба. Определяме риска от злоупотреба въз основа на различни фактори, включително, но не само, жалби за конкретни приложения и програмисти, новини, предишни нарушения, отзиви от потребители и използване на популярни марки, персонажи и други активи.

Как работи Google Play Protect

Google Play Protect проверява приложенията при инсталирането им. Също така функцията периодично сканира устройството ви. Ако намери потенциално опасно приложение, може да направи следното:

- Да ви изпрати известие. За да премахнете приложението, докоснете известието, след което – „Деинсталиране“.
- Да деактивира приложението, докато не го деинсталирате.
- Да премахне приложението автоматично. В повечето случаи при откриването на опасно приложение ще получите известие, че то е премахнато.

Как работи защитата от злонамерен софтуер

За да ви предпазва от злонамерен софтуер на трети страни, опасни URL адреси и групи проблеми със сигурността, Google може да получава информация за:

- мрежовите връзки на устройството ви;
- потенциално опасни URL адреси;
- операционната система на устройството ви, както и за приложенията, инсталирани на него чрез Google Play или от други източници.

Възможно е да получите предупреждение от Google за потенциално опасни приложения или URL адреси. Те може да бъдат премахнати или блокирани от Google, ако е известно, че са опасни за устройства, данни или потребители.

Можете да деактивирате някои от тези защити от настройките на устройството си. Възможно е обаче Google да продължи да получава информация за приложенията, инсталирани чрез Google Play, а тези, инсталирани на устройството ви от други източници, може да продължат да бъдат проверявани за проблеми със сигурността, без да се изпраща информация до Google.

Как работят сигналите за поверителност

Google Play Protect ще ви изпрати сигнал, ако дадено приложение бъде премахнато от Google Play Магазин, защото може да осъществява достъп до личната ви информация. Ще имате възможност да деинсталирате съответното приложение.

Прилагане на правилата

Когато преглеждаме съдържание или профили, за да определим дали са незаконни и да решим дали нарушават правилата ни, вземаме под внимание различна информация, включително метаданните на приложението (например заглавие на приложението, описание), практическата работа в приложението, информация за профила (напр. предишна история на нарушения на правилата), код на трета страна, използван в приложения, и други данни, предоставени чрез механизми за подаване на сигнали (където е приложимо) и проверки по собствена инициатива. Имайте предвид, че е ваша отговорност да гарантирате, че кодът на трета страна (например SDK), използван в приложението ви, както и практиките на третата страна по отношение на приложението ви спазват всички програмни правила за програмистите в Google Play.

Ако приложението или профилът ви на програмист нарушават някои от правилата ни, ще предприемем съответните мерки, които са описани по-долу. Освен това ще ви предоставим по имейл необходимата информация за предприетите мерки, както и инструкции за обжалване, ако смятате, че сме допуснали грешка.

Моля, обърнете внимание, че с премахването или административните известия може да не се посочи всяко нарушение на правилата от страна на профила ви, приложението ви или на по-широката ви гама от приложения. Задължение на програмистите е да решат всеки проблем с правилата и да положат дължимите допълнителни грижи, за да гарантират, че

останалата част от приложението или профила им спазват всички правила. Ако не отстраните нарушенията на правилата в профила си и във всичките си приложения, това може да доведе до предприемането на допълнителни мерки.

Многократни или сериозни нарушения (като например злонамерен софтуер, измама и приложения, които могат да навредят на потребителите или устройствата) на тези правила или на [Споразумението с програмистите относно разпространението](#) ще доведат до прекратяването на отделни или свързани профили на програмисти в Google Play.

Наложени мерки

Различните действия по налагане на мерки могат да засегнат приложенията ви по различни начини. Извършваме проверки с помощта на хора и автоматизирани инструменти, за да преглеждаме приложенията и съдържанието в тях така, че да откриваме и оценяваме нарушаващото правилата съдържание, което е опасно за потребителите и за екосистема на Google Play. Използването на автоматизирани модели ни помага да откриваме повече нарушения и по-бързо да оценяваме потенциалните проблеми. Така запазваме услугата Google Play безопасна за всички. Нарушаващото правилата съдържание се премахва от автоматизираните ни модели или, ако е нужно по-задълбочено решение, се означава за допълнителна проверка от обучени оператори и анализатори, които го оценяват (например когато е необходимо разбиране на контекста на съдържанието). Резултатите от тези ръчни проверки след това се използват в помощ на изграждането на данни за обучение за по-нататъшно подобряване на моделите ни за машинно обучение.

В следващата секция се описват различните действия, които Google Play може да предприеме, както и въздействието върху приложението ви и/или профила ви на програмист в услугата.

Тези действия засягат всички региони, освен ако не е посочено друго в съобщението за наложени мерки. Ако например приложението ви е спряно, то ще бъде недостъпно във всички региони. В допълнение тези мерки ще останат в сила, докато не ги обжалвате и обжалването ви не бъде одобрено, освен ако не е посочено друго.

Отхвърляне

- Новите приложения или актуализации на приложения, изпратени за преглед, няма да бъдат налице в Google Play.
- Ако актуализацията на съществуващо приложение бъде отхвърлена, публикуваната преди актуализацията версия ще остане налице в Google Play.
- Отхвърлянията не оказват влияние върху достъпа ви до съществуващите инсталирания от потребители, статистически данни и оценки за отхвърленото приложение.
- Отхвърлянията не оказват влияние върху реномето на профила ви на програмист в Google Play.

Забележка: Не опитвайте да изпратите отново отхвърлено приложение, докато не коригирате всички нарушения на правилата.

Премахване

- Приложението, както и всичките му предишни версии, се премахват от Google Play и повече няма да са налице за изтегляне от потребителите.
- Тъй като приложението е премахнато, потребителите няма да виждат малката му обява в магазина. Тази информация ще бъде възстановена, когато изпратите актуализация за премахнатото приложение, която е в съответствие с правилата.
- Потребителите може да нямат възможност да извършват покупки в приложението или да използват функциите за въградено таксуване, докато спазваща правилата версия не бъде

одобрена от Google Play.

- Премахванията не оказват незабавно влияние върху реномето на профила ви на програмист в Google Play, но многобройните премахвания може да доведат до спиране.

Забележка: Не опитвайте да публикувате повторно премахнатото приложение, докато не коригирате всички нарушения на правилата.

Спиране на профила

- Приложението, както и всичките му предишни версии се премахват от Google Play и повече няма да са налице за изтегляне от потребителите.
- Спирането може да е в резултат на груби или многобройни нарушения на правилата, както и на неколкостепенното отхвърляне или премахване на приложението.
- Тъй като приложението е спряно, потребителите няма да виждат малката му обява в магазина.
- Повече не можете да използвате APK файла или пакета Android App Bundle на спряното приложение.
- Потребителите няма да могат да извършват покупки в приложението или да използват функциите на услугата за въграден таксуване.
- Спиранята са в ущърб на доброто реноме на профила ви на програмист в Google Play, а многобройните предупреждения могат да доведат до прекратяването на отделни или свързани профили.

Ограничена видимост

- Откриваемостта на приложението ви в Google Play е ограничена. Приложението ви ще остане налично в Google Play и потребителите ще имат достъп до него чрез директна връзка към малката му обява в магазина.
- Ограничаването на видимостта на приложението ви не оказва влияние върху реномето на профила ви на програмист в Google Play.
- Ограничаването на видимостта на приложението ви не оказва влияние върху възможността на потребителите да виждат съществуващата му малка обява в магазина.

Ограничени региони

- Приложението ви може да бъде изтеглено от потребителите с помощта на Google Play само в определени региони.
- Потребителите от други региони няма да могат да намерят приложението в Google Play Магазин.
- Потребителите, които са инсталирали приложението преди това, могат да продължат да го използват на устройството си, но няма да получават повече актуализации.
- Ограничението за региони не оказва влияние върху реномето на профила ви на програмист в Google Play.

Ограничен профил

- Когато профилът ви на програмист бъде ограничен, всички приложения в каталога ви ще бъдат премахнати от Google Play и повече няма да можете да публикувате нови приложения, нито да публикувате повторно съществуващи. Пак ще имате достъп до Play Console.
- Тъй като всички приложения са премахнати, потребителите няма да виждат малките им обяви в магазина и потребителския ви профил на програмист.
- Текущите ви потребители няма да могат да извършват покупки в приложенията или да използват функциите на услугата за въграден таксуване.

- Пак можете да използвате Play Console, за да предоставите повече информация на Google Play и да промените данните за профила си.
- Ще имате възможност да публикувате повторно приложенията си, след като коригирате всички нарушения на правилата.

Прекратяване на профил

- Когато профилът ви на програмист бъде прекратен, всички приложения в каталога ви ще бъдат премахнати от Google Play и повече няма да можете да публикувате нови. Това означава и че всички свързани профили на програмист в Google Play също ще бъдат спрени за постоянно.
- Многобройните спирания или такива за груби нарушения на правилата могат да доведат до прекратяването на профила ви в Play Console.
- Тъй като приложенията в прекратения профил са премахнати, потребителите няма да могат да виждат малките им обяви в магазина и потребителския ви профил на програмист.
- Текущите ви потребители няма да могат да извършват покупки в приложенията или да използват функциите на услугата за въградено таксуване.

Забележка: Всеки нов профил, който опитате да отворите, също ще бъде прекратен (без възстановяване на регистрационната такса за програмист), затова, моля, не опитвайте да си регистрирате нов профил в Play Console, докато някой от другите ви е прекратен.

Неактивни профили

Неактивните профили са профили на програмисти, които не са активни или са изоставени. Неактивните профили не са с добро реноме, както се изисква в [Споразумението с програмистите относно разпространението](#).

Профилите на програмист в Google Play трябва да бъдат използвани от активни програмисти, които публикуват и поддържат приложенията си. С цел предотвратяване на злоупотреби закриваме профилите, които са неактивни, не са използвани или с тях не се работи редовно, като например за публикуване и актуализиране на приложения, осъществяване на достъп до статистически данни или управление на малките обяви в магазина.

При [закриването на неактивен профил](#) той и всички свързани с него данни ще бъдат изтрити. Таксата ви за регистрация не подлежи на възстановяване и ще бъде загубена. Преди да закроем неактивния ви профил, ще ви уведоим посредством предоставената за него информация за връзка.

Закриването на неактивен профил няма да ограничи възможността ви да си създадете нов профил впоследствие, в случай че решите да публикувате в Google Play. Няма да можете да активирате повторно профила си и предишните ви приложения и данни няма да бъдат достъпни в новия профил.

Справяне с нарушенията на правилата и подаване на сигнали за тях

Обжалване на наложени мерки

Ако е била допусната грешка и установим, че приложението ви не нарушава програмните правила на Google Play и Споразумението с програмистите относно разпространението, ще го възстановим. В случай че сте прегледали внимателно правилата и смятате, че е възможно да сме допуснали грешка, моля, изпълнете инструкциите, предоставени в имейл с

известие за наложена мярка, за да обжалвате решението ни или [кликнете тук](#), за да обжалвате решението ни.

Допълнителни ресурси

Ако ви е необходима още информация относно наложени мерки или оценка/коментар от потребител, може да разгледате някои от ресурсите по-долу или да се свържете с нас чрез [Помощния център на Google Play](#). Не можем обаче да ви дадем юридически съвет. В случай че имате нужда от такъв, моля, обърнете се към правен експерт.

- [Удостоверяване на приложения](#)
 - [Подаване на сигнал за нарушение на правилата](#)
 - [Свързване с Google Play относно прекратяване на профил или премахване на приложение](#)
 - [Справедливи предупреждения](#)
 - [Подаване на сигнали за неподходящи приложения и коментари](#)
 - [Приложението ми е премахнато от Google Play](#)
 - [Запознаване с прекратяването на профили на програмисти в Google Play](#)
-

Изисквания на Play Console

За да гарантираме безопасността и сигурността на колеритната ни екосистема от приложения, Google Play изисква всички програмисти да изпълнят изискванията на Play Console, включително всички потребителски профили, които са свързани с профила на програмист в Play Console. Потвърдената информация ще се показва в Google Play, така че потребителите да изградят доверие към програмистите. [Научете повече за информацията, която се показва в Google Play](#).

Google Play предлага два типа профил на програмист – личен и на организация. Изборът на правилния тип профил на програмист и завършването на необходимите стъпки за потвърждаване са от ключово значение за безпроблемното включване. [Научете повече за избора на тип профил на програмист](#).

Когато създават профила си в Play Console, програмистите, които предоставят следните услуги, трябва да се регистрират като организация:

- финансови продукти и услуги, включително, без изброяването да е изчерпателно, банкиране, заеми, борсова търговия, инвестиционни фондове, софтуерни портфейли и борси за криптовалути. [Научете повече за правилата относно финансовите услуги](#).
- здравни приложения, като например приложения за медицина и такива за проучвания с хора. [Научете повече за категориите здравни приложения](#).
- приложения, които са одобрени да използват класа [VpnService](#) . [Научете повече за правилата относно VPN услугите](#).
- правителствени приложения, включително такива, които са разработени от правителствен орган или от името на такъв.

След като изберете типа профил, трябва:

- да посочите точно информацията за профила си на програмист, включително следните подробности:
 - пълно име и адрес;
 - [DUNS номер](#) , ако се регистрирате като организация;
 - имейл адрес и телефонен номер за връзка;
 - показваните в Google Play имейл адрес и телефонен номер на програмиста, когато е приложимо;
 - начини на плащане, когато е приложимо;

- потребителски профил за плащания чрез Google, свързан с профила ви на програмист.
- ако се регистрирате като организация, информацията в профила ви на програмист трябва да е актуална и да съответства на подробностите в потребителския ви профил в Dun & Bradstreet.

Преди да изпратите приложението си, трябва:

- да предоставите точна и пълна информация и метаданни за него;
- да качите декларацията му за поверителност и да попълните секцията за безопасност на данните;
- да предоставите активен демонстрационен профил, данни за вход и всички останали ресурси, необходими за прегледа на приложението ви от Google Play (по-конкретно, [идентификационни данни за вход](#), QR код и др.).

Както винаги, приложението ви трябва да е стабилно, да работи бързо и да е интригуващо за потребителите. Проверете отново дали всичките му компоненти, включително рекламните мрежи, услугите за анализ и SDK на трети страни, спазват [програмните правила за програмистите](#) в Google Play. Ако целевата аудитория на приложението ви включва деца, то трябва да спазва и [правилата за семейства](#).

Не забравяйте, че е ваше задължение да прегледате [Споразумението с програмистите относно разпространението](#) и всички [програмни правила за програмистите](#), за да се уверите, че приложението ви отговаря на всички изисквания.

[Developer Distribution Agreement](#)

Нуждаете се от още помощ?

Изпробвайте следните стъпки:



Свържете се с нас

Кажете ни повече и ще ви помогнем