개발자 프로그램 정책

(달리 명시되지 않는 한 2025년 4월 10일부터 시행)

앱과 게임 분야에서 가장 신뢰할 수 있는 스토어가 되도록 도와주세요.

혁신적인 기술은 개발자와 Google 모두에게 성공을 의미하지만, 거기에는 책임도 따르기 마련입니다. 개발자 프로그램 정책과 개발자 배포 계약은 Google Play를 통해 십억 명 이상의 사용자에게 전 세계에서 가장 혁신적이고 신뢰할 수 있는 앱을 계속 제공하기 위해 마련되었습니다. 아래에서 정책을 살펴보시기 바랍니다.

제한된 콘텐츠

전 세계 사용자가 매일 Google Play를 통해 앱 및 게임에 액세스합니다. 앱을 제출하기 전에 앱이 Google Play에 적합하며 현지 법률을 준수하는지 확인하세요.

아동 학대

아동 착취 또는 학대를 조장하는 콘텐츠의 제작, 업로드 또는 배포를 금지하지 않는 앱은 Google Play에서 즉시 삭제됩니다. 여기에는 모든 아동 성적 학대 콘텐츠가 포함됩니다. 아동 착취의 가능성이 있는 콘텐츠를 Google 제품에서 발견한 경우 이를 신고하려면 **악용사례 신고** 를 클릭하세요. Google이 아닌 다른 인터넷 사이트에서 이러한 콘텐츠를 발견하는 경우 거주 국가의 해당 기관 에 직접 문의하시기 바랍니다.

아동을 위험에 처하게 하는 앱 사용은 금지됩니다. 여기에는 다음과 같이 아동에 대한 약탈적 행위를 조장하는 앱 사용이 포함되며 이에 국한되지 않습니다.

- 아동을 대상으로 하는 부적절한 상호작용(예: 더듬거나 애무하는 행위)
- 아동 그루밍(예: 온라인을 통해 아동과 친구가 된 다음 온라인 또는 오프라인에서 해당 아동과의 성적 접촉 및/또는 성적인 이미지 교환을 조장하는 행위)
- 미성년자의 성적 대상화(예: 아동 성적 학대를 묘사, 조장 또는 선동하는 이미지 또는 아동의 성적 착취를 야기할 수 있는 방식의 아동 묘사)
- 성 착취(예: 아동의 사적인 이미지에 실제로 접근하거나 접근할 수 있다고 주장하여 아동에게 위협이나 협박을 가하는 행위)
- 아동 인신매매(예: 상업적 목적의 아동 성 착취에 관한 광고 또는 제안)

아동 성적 학대 콘텐츠를 인지하게 되면 Google은 미국 국립실종학대아동센터(National Center for Missing & Exploited Children: NCMEC)에 신고하는 등 적절한 조치를 취합니다. 아동이 학대, 착취 또는 인신매매의 위험에 처해 있거나 피해를 입었다고 판단되는 경우 현지 법 집행 기관과 여기 에 명시된 아동 보호 기관에 신고하시기 바랍니다.

아동의 관심을 유도하지만 성인용 주제가 포함된 앱 또한 허용되지 않으며, 이러한 앱은 다음을 포함하되 이에 국한되지 않습니다.

- 과도한 폭력, 피, 신체 훼손 등 잔인한 콘텐츠가 포함된 앱
- 유해하고 위험한 활동을 묘사하거나 조장하는 앱

또한 미용상의 목적으로 이루어지는 성형수술, 체중 감량, 기타 외모 관련 미용 시술을 묘사하는 앱을 비롯해 부정적인 신체 이미지 또는 자아상을 조장하는 앱도 허용되지 않습니다.

아동 안전 표준 정책

Google Play는 소셜 및 데이트 앱에 Google 아동 안전 표준 정책을 준수할 것을 요구합니다.

이러한 앱은 다음을 충족해야 합니다.

- **표준 게시:** 앱은 앱의 서비스 약관, 커뮤니티 가이드 또는 기타 공개적으로 제공되는 사용자 정책 문서와 같이 공개적으로 액세스 가능한 표준을 통해 아동 성적 학대 및 착취(CSAE: Child Sexual Abuse and Exploitation)를

명시적으로 금지해야 합니다.

- **사용자 의견을 제공할 수 있는 인앱 메커니즘 제공:** 사용자가 앱에서 의견, 우려사항 또는 신고를 제출할 수 있도록 앱 내에서 메커니즘을 제공함을 자체적으로 인증해야 합니다.
- **CSAM(Child Sexual Abuse Materials) 처리:** 게시된 표준 및 관련 법규에 따라 앱이 적절한 조치를 취하고 있음을 자체적으로 인증해야 합니다. 여기에는 CSAM을 실제로 인지한 후 삭제하는 조치를 포함하나 이에 국한되지 않습니다.
- **어린이 안전 법규 준수:** 앱이 관련 어린이 안전 법률 및 규정을 준수함을 자체적으로 인증해야 합니다. 여기에는 확인된 CSAM을 국립 실종학대아동방지센터 또는 관련 지역 당국에 신고하는 절차의 마련을 포함하되 이에 국한되지 않습니다.
- **어린이 안전 담당자 지정:** 앱에는 앱 또는 플랫폼에서 발견된 CSAE 콘텐츠에 관해 Google Play가 보낼 수 있는 알림을 받을 담당자가 지정되어 있어야 합니다. 이 담당자는 시행 및 검토 절차에 관해 논의하고 필요시 조치를 취할 수 있는 직책이어야 합니다.

고객센터 도움말에서 이 요구사항과 준수 방법을 자세히 알아보세요.

부적절한 콘텐츠

Google Play가 안전하고 건전한 플랫폼이 될 수 있도록 Google은 사용자에게 유해하거나 부적절한 콘텐츠를 정의하고 금지하는 표준을 마련했습니다.

성적인 콘텐츠 및 욕설

음란물을 비롯한 성적인 콘텐츠나 욕설 또는 성적 만족을 주기 위한 콘텐츠나 서비스를 포함하거나 홍보하는 앱은 허용되지 않습니다. 보상을 대가로 제공하는 성적인 행위를 홍보하거나 조장하는 것으로 해석되는 앱 또는 앱 콘텐츠는 허용되지 않습니다. 성적 약탈 행위와 관련된 콘텐츠를 포함 또는 홍보하거나 동의 없이 성적인 콘텐츠를 배포하는 앱은 허용되지 않습니다. 과도한 노출이 포함된 콘텐츠는 교육, 다큐멘터리, 과학 또는 예술이 주목적이며 불필요한 노출이 포함되지 않은 경우 허용될 수 있습니다.

더 광범위한 콘텐츠 카탈로그에 포함된 도서/동영상을 열거하는 앱인 카탈로그 앱은 다음 요건을 충족하는 경우 성적인 콘텐츠가 포함된 도서(eBook 및 오디오북 포함) 또는 동영상을 배포할 수 있습니다.

- 성적인 콘텐츠가 포함된 도서/동영상이 앱의 전체 카탈로그 중 미미한 부분을 차지합니다.
- 앱에서 성적인 콘텐츠가 포함된 도서/동영상을 적극적으로 홍보하지 않습니다. 사용자 기록을 바탕으로 또는 일반 가격 프로모션 중에 이러한 콘텐츠가 추천에 표시될 수 있습니다.
- 앱에서 아동 학대 콘텐츠, 포르노 또는 관련 법률에 따라 불법으로 규정된 기타 성적인 콘텐츠가 포함된 도서/동영상을 배포하지 않습니다.
- 앱에서 성적인 콘텐츠가 포함된 도서/동영상 액세스를 제한하여 미성년자를 보호합니다.

앱에 이 정책을 위반하는 콘텐츠가 포함되어 있지만 해당 콘텐츠가 특정 지역에서 적절하다고 간주되는 경우 해당 지역의 사용자는 앱을 사용할 수 있지만 다른 지역의 사용자는 사용할 수 없습니다.

다음은 자주 발생하는 위반 사례입니다.

- 대상이 옷을 입지 않고 있거나 흐리게 처리되어 있거나 최소한의 옷만을 입고 있거나 공공장소에 적합하지 않은 옷을 입고 있는 성적인 노출 또는 선정적인 자세의 묘사
- 성행위 또는 선정적인 자세를 묘사하거나 신체 부위를 성적으로 묘사하는 애니메이션 또는 삽화
- 기능적으로 성행위를 보조하는 기구, 성행위 가이드, 불법인 성적 테마, 페티시 또는 이를 묘사하는 콘텐츠
- 음란하거나 욕설이 포함된 콘텐츠. 스토어 등록정보 또는 앱 내에 욕설, 비방, 음란한 표현이나 성인용/성적인 키워드를 포함하는 콘텐츠를 포함하되 이에 국한되지 않습니다.
- 수간을 묘사, 설명 또는 조장하는 콘텐츠
- 성 관련 유흥, 성매매 알선 또는 보상을 대가로 성적인 행위를 제공하는 것으로 해석될 수 있는 기타 서비스를 홍보하거나 조장하는 앱. 일방 당사자가 현금, 선물 또는 재정적 지원을 상대방에게 제공하는 것으로 예상 또는 암시되는 조건 만남 또는 성매매 알선('원조교제')을 포함하되 이에 국한되지 않습니다.
- 장난 또는 엔터테인먼트 앱이라는 라벨이 지정되었더라도 사람들을 비하하거나 대상화하는 앱(예: 사람들의 옷을 벗기거나 옷을 입은 상태에서도 벌거벗은 몸을 볼 수 있다고 주장하는 앱)

- 불법 촬영, 몰래카메라, 딥페이크나 기타 유사한 기술로 동의 없이 제작한 성적인 콘텐츠같이 성적인 방식으로 사람을 위협하거나 착취하려는 콘텐츠 또는 행위

증오심 표현

인종 또는 민족, 종교, 장애, 연령, 국적, 군필 여부, 성적 지향, 성별, 성 정체성, 계급, 이민 상태 또는 제도적 차별이나 소외의 대상이 될 수 있는 기타 특성을 근거로 특정 개인이나 집단을 상대로 한 폭력이나 증오심을 조장하는 앱은 허용되지 않습니다.

나치와 관련된 EDSA(교육, 다큐멘터리, 과학, 예술) 콘텐츠를 포함한 앱은 현지 법률 및 규정에 따라 일부 국가에서 차단될 수 있습니다.

다음은 자주 발생하는 위반 사례입니다.

- 보호 대상 집단이 비인간적이거나 열등하거나 증오의 대상임을 주장하는 콘텐츠 또는 발언
- 보호 대상 집단이 부정적인 특성(예: 악의적임, 부패함, 악함 등)을 가지고 있다는 혐오 발언, 편견 또는 이론을 포함하거나, 해당 집단이 위협이 된다고 명시적 또는 암묵적으로 주장하는 앱
- 특정 개인이 보호 대상 집단의 일원이기 때문에 증오나 차별의 대상이 되어야 한다고 다른 사람이 생각하도록 조장하는 콘텐츠나 발언
- 깃발, 상징물, 휘장, 용품과 같은 혐오의 상징 또는 혐오 집단과 관련된 행동을 조장하는 콘텐츠

폭력

지나친 폭력 또는 기타 위험한 행위를 묘사하거나 조장하는 앱은 허용되지 않습니다. 만화, 사냥, 낚시와 같은 오락 맥락에서 가상의 폭력을 묘사하는 앱은 일반적으로 허용됩니다.

다음은 자주 발생하는 위반 사례입니다.

- 사람 또는 동물에 대한 사실적인 폭력이나 폭력적 위협을 생생하게 묘사하거나 설명합니다.
- 자해, 자살, 섭식장애, 질식 게임 또는 심각한 부상이나 죽음으로 이어질 수 있는 기타 행위를 조장하는 앱입니다.

폭력적 극단주의

민간인을 상대로 한 폭력 행위에 가담했거나, 이를 준비했거나, 자행했다고 주장하는 테러 조직이나 기타 위험한 조직 또는 운동은 조직원 모집을 비롯한 어떤 목적으로도 Google Play에 앱을 게시할 수 없습니다.

Google은 폭력적 극단주의와 관련된 콘텐츠나 테러 행위 조장, 폭력 선동, 테러 공격 기념 등 민간인을 대상으로 한 폭력을 계획, 준비 또는 미화하는 콘텐츠가 포함된 앱을 허용하지 않습니다. 교육, 다큐멘터리, 과학 또는 예술(EDSA) 목적으로 폭력적 극단주의와 관련된 콘텐츠를 게시하는 경우, 관련된 EDSA 맥락을 충분히 제공하시기 바랍니다.

민감한 사건

국내 비상 사태, 자연재해, 공중보건 비상 사태, 물리적 충돌, 죽음 또는 기타 비극적인 사건과 같이 사회, 문화 또는 정치적으로 막대한 영향을 미치는 민감한 사건을 이용하여 수익을 창출하거나 이러한 사건을 부적절하게 다루는 앱은 허용되지 않습니다. 민감한 사건 관련 콘텐츠가 포함된 앱은 콘텐츠에 EDSA(교육, 다큐멘터리, 과학, 예술)로서의 가치가 있거나 사용자를 대상으로 민감한 사건에 관해 알리고 인식을 고취하려는 목적이 있는 경우 일반적으로 허용됩니다.

다음은 자주 발생하는 위반 사례입니다.

- 자살, 약물 과다 복용, 자연적 원인 등으로 인한 실제 인물 혹은 집단의 죽음과 관련하여 둔감하고 무례하게 발언하는 행위
- 분명하게 문서로 기록되어 있는 대형 참사의 발생 사실을 부정하는 행위
- 희생자들에게 돌아가는 뚜렷한 혜택 없이 민감한 사건을 이용하여 이득을 취하려는 행위

따돌림 및 괴롭힘

위협, 괴롭힘, 따돌림을 포함하거나 조장하는 앱은 허용되지 않습니다.

다음은 자주 발생하는 위반 사례입니다.

- 국제적 또는 종교적 갈등의 피해자들을 괴롭히는 행위.
- 갈취, 협박 등을 포함하여 다른 사람을 이용하려는 콘텐츠
- 누군가를 공개적으로 모욕하기 위해 콘텐츠를 게시
- 비극적 사건의 피해자나 피해자의 가족 및 지인을 괴롭히는 행위.

위험한 제품

폭발물, 총기, 탄약, 특정 총기 부대용품의 판매를 촉진하는 앱은 허용되지 않습니다.

- 제한된 액세서리에는 총기에서 자동 발사를 시뮬레이션할 수 있게 해 주거나 총기를 자동 발사 화기로 바꿔주는 액세서리(예: 범프스톡, 개틀링 트리거, 드롭인 오토 시어스, 컨버전 키트) 및 30회 이상 발사가 가능한 탄창 또는 벨트가 포함됩니다.

폭발물, 총기, 탄약, 제한된 총기 액세서리, 기타 무기의 제조 방법을 설명하는 앱은 허용되지 않습니다. 여기에는 총기를 자동 발사 또는 시뮬레이션 자동 발사 총기로 바꾸는 방법도 포함됩니다.

마리화나

적법성과 관계없이 마리화나 또는 마리화나 제품의 판매를 조장하는 앱은 허용되지 않습니다.

다음은 자주 발생하는 위반 사례입니다.

- 사용자가 인앱 장바구니 기능을 통해 마리화나를 주문하도록 허용합니다.
- 사용자가 마리화나를 배달하거나 전달받을 수 있도록 지원합니다.
- THC(테트라히드로칸나비놀) 함유 CBD 오일과 같이 THC가 함유된 제품 판매를 조장합니다.

담배 및 주류

담배 또는 니코틴이 포함된 제품(예: 전자 담배, 액상형 전자 담배, 니코틴 파우치)의 판매를 촉진하거나 알코올, 담배 또는 니코틴을 불법적이거나 부적절하게 사용하도록 조장하는 앱은 허용되지 않습니다.

추가 정보

- 미성년자를 대상으로 주류 또는 담배의 사용 또는 판매를 묘사하거나 조장해서는 안 됩니다.
- 담배 소비가 사회적 또는 직업적 평판이나 지적, 성적 또는 신체적 기능을 향상할 수 있다고 암시해서는 안 됩니다.
- 과음, 폭음 또는 음주 경쟁을 긍정적으로 묘사하는 등 과도한 음주를 긍정적으로 묘사해서는 안 됩니다.
- 담배 제품을 광고하거나, 홍보하거나, 눈에 잘 띄는 곳에 표시(광고, 배너, 카테고리뿐만 아니라 담배 판매 사이트로 연결되는 링크 포함)해서는 안 됩니다.
- 특정 지역의 음식/식료품 배달 앱의 경우 담배 제품의 판매가 제한적으로 허용될 수 있으며, 연령 제한 보호 장치(예: 배달 시 신분증 확인)가 적용됩니다.
- 연령 제한 보호 장치가 있는 경우 니코틴 사용 중단을 위한 지원 도구로 홍보되는 제품의 판매는 허용될 수 있습니다.

금융 서비스

사기성이 있거나 유해한 금융 상품 및 서비스에 사용자를 노출하는 앱은 허용되지 않습니다.

이 정책의 목적상 금융 상품 및 서비스란 맞춤 재무 컨설팅을 포함한 자금 및 암호화폐의 관리 또는 투자와 관련된 상품 및 서비스를 의미합니다.

앱에 금융 상품 및 서비스가 포함되어 있거나 앱에서 금융 상품 및 서비스를 홍보하는 경우 앱이 대상으로 하는 모든 지역 또는 국가의 주정부 및 현지 규정(예: 현지 법규에서 요구하는 특정 공개 요건)을 준수해야 합니다.

금융 기능이 포함된 모든 앱은 Play Console 내에서 금융 기능 선언 양식을 작성해야 합니다.

바이너리 옵션

사용자에게 바이너리 옵션을 거래하는 기능을 제공하는 앱은 허용되지 않습니다.

대출

개인 대출: 개인 대출이란 한 개인, 조직, 법인이 고정 자산 구매 또는 교육 자금을 조달하는 것 이외의 목적으로 개별 소비자에게 단발적으로 돈을 빌려주는 것을 의미합니다. 개인 대출 상품을 이용하려는 소비자가 이용 여부에 관한 정확한 판단을 내리기 위해서는 대출 상품의 건전성, 특징, 수수료, 상환 일정, 위험, 혜택에 관한 정보를 알고 있어야 합니다.

- 예: 개인 대출, 급여 담보 대출, P2P 대출, 자동차 담보 대출
- 예외: 모기지론, 자동차 구매 자금 대출, 리볼빙 신용 한도(신용카드, 개인 신용 한도 등)

급여 선지급: 급여 선지급 대출(EWA)은 개인이 이미 획득했으나 고용주가 아직 지급하지 않은 급여의 일부를 이용할 수 있도록 하는 금융 서비스입니다. 기존 대출과 달리 EWA 서비스에는 다음과 같은 특징이 있습니다.

- 상환 메커니즘: 급여 공제 또는 사용자의 은행 계좌에 연결된 자동 결제 거래를 통해 상환이 자동으로 발생합니다. 자동 결제 거래에 실패할 경우 추가 이자, 벌금 또는 수수료가 부과되지 않습니다.
- 수입 기반 접근: 사용자에게 제공되는 금액은 현재 급여 지급 주기에 사용자가 이미 획득한 임금으로 엄격하게 제한되며, 향후 수입을 담보로 대출할 수는 없습니다.
- 수수료 구조: EWA 서비스는 이자를 부과하지 않는 대신 사용에 따른 소액의 정액 수수료 또는 비율 기준 거래 수수료를 부과합니다. 합리적인 수수료는 최소한으로 투명하게 부과되며, 사용자에게 부담을 지우지 않고 서비스를 제공하는 실제 비용을 반영하여 보통 거래당 1~5달러 또는 선지급금의 1~5% 수준에서 책정됩니다.
- 부채 창출 없음: EWA 서비스는 일반적으로 거래를 신용 기관에 신고하지 않으므로 사용자의 신용 점수에 영향을 미치거나 장기적인 부채 축적에 기여하지 않습니다.

개인 대출을 제공하는 앱(직접 대출을 제공하는 앱, 리드 생성기, 소비자를 제3자 대출 기관과 연결해 주는 앱을 포함하되 이에 국한되지 않음)은 앱 메타데이터에 다음 정보를 반드시 공개해야 하며, Play Console에서 앱 카테고리가 '금융'으로 설정되어 있어야 합니다.

- 최단/최장 상환 기간
- 일반적으로 1년 동안의 이율과 수수료 및 기타 비용이 포함된 최대 연이율(APR) 또는 현지 법률에 따라 계산된 유사한 기타 이율
- 원금 및 모든 관련 수수료가 포함된 총대출 비용의 대표적인 예시
- 개인 정보 및 민감한 사용자 데이터에 대한 액세스, 수집, 사용, 공유(이 정책에 명시된 제한사항이 적용됨)를 포괄적으로 공개하는 개인정보처리방침

대출이 이루어진 날로부터 60일 이내에 전액 상환을 요구하는 개인 대출('단기 개인 대출'이라고 지칭)을 홍보하는 앱은 허용되지 않습니다.

정립된 법적 체계에 따라 구체적인 규정을 통해 그러한 단기 대출 관행을 명시적으로 허용하는 국가 내에서 운영되는 개인 대출 앱에는 본 정책의 예외가 고려됩니다. 이와 같이 드문 경우에는 해당 국가의 관련 현지 법률 및 규정 가이드라인에 따라 예외 적용 여부를 평가합니다.

급여 선지급 대출을 제공하는 앱(직접 대출을 제공하는 앱, 리드 생성기, 소비자와 서드 파티 대출 기관을 연결해 주는 앱을 포함하되 이에 국한되지 않음)은 Play Console에서 앱 카테고리를 '금융'으로 설정하고 앱 메타데이터에 다음 정보를 공개해야 합니다.

- 상환 기간 및 조건
- 구독료, 거래 수수료, 대출 제공과 관련된 다른 모든 수수료를 포함한 모든 수수료
- 수수료가 모두 포함된 총 대출 비용 예시
- 개인 정보 및 민감한 사용자 데이터에 대한 액세스, 수집, 사용, 공유(이 정책에 명시된 제한사항이 적용됨)를 포괄적으로 공개하는 개인정보처리방침

개인 대출 서비스 제공 자격 증명을 위해 제출된 라이선스 또는 서류와 귀하의 개발자 계정과의 연관 관계를 Google에서 확인할 수 있어야 합니다. 계정이 모든 현지 법률 및 규정을 준수하는지 확인하기 위해 추가 정보 또는 문서를 요청할 수 있습니다.

개인 대출 앱, 개인 대출 알선이 주목적인 앱(예: 리드 생성기 또는 알선자), 부수적인 대출 앱(대출 계산기, 대출 가이드 등), Earned Wage Access(EWA) 앱은 사진이나 연락처 같은 민감한 정보에 대한 액세스가 금지됩니다. 다음 권한은 금지됩니다.

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

민감한 정보 또는 API를 활용하는 앱에는 추가 제한사항 및 요구사항이 적용됩니다. 자세한 내용은 권한 정책을 참고하세요.

고금리 개인 대출

미국에서는 연이율(APR)이 36% 이상인 개인 대출용 앱이 허용되지 않습니다. 미국의 개인 대출용 앱은 공정대부법(TILA, Truth in Lending Act) 에 따라 계산된 최대 APR을 표시해야 합니다.

이 정책은 대출을 직접 제공하는 앱, 리드 생성기, 소비자를 제3자 대출 기관과 연결해 주는 경우에 적용됩니다.

국가별 요건

목록에 기재된 국가를 타겟팅하는 개인 대출 앱은 추가 요건을 준수해야 하며, Play Console 내에서 금융 기능 선언의 일환으로 추가 문서를 제공해야 합니다. 급여 선지급 대출(EWA)을 제공하는 앱에는 관련 관할에서 해당하는 범위 내에서 이러한 요구사항이 적용됩니다. Google Play의 요청에 따라 관련 규정 및 라이선스 요건 준수에 관한 추가 정보 또는 문서를 제공해야 합니다.

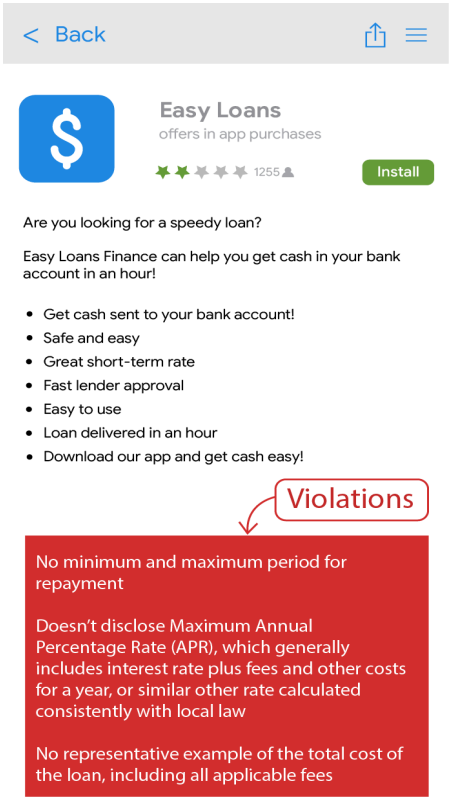
1. **인도**
   - 인도중앙은행(RBI)으로부터 개인 대출을 제공하기 위한 라이선스를 받은 경우 검토를 위해 라이선스 사본을 제출해야 합니다.
   - 대출 활동에 직접 참여하지는 않으며 등록된 비은행 금융회사(NBFC) 또는 은행의 대출을 지원하는 플랫폼만 제공한다면 선언에 이를 정확히 명시해야 합니다.
     - 또한 등록된 모든 NBFC 및 은행의 이름을 앱 설명에 명시적으로 공개해야 합니다.
2. **인도네시아**
   - 앱이 OJK 규정 제77/POJK.01/2016(경우에 따라 개정될 수 있음)에 따른 정보 기술 기반 대출 서비스 활동에 관여하는 경우 유효한 라이선스 사본을 제출해 검토를 받아야 합니다.
3. **필리핀**
   - 온라인 대출 플랫폼(OLP)을 통해 대출을 제공하는 모든 금융 및 대출 기업은 필리핀 증권거래위원회(PSEC)에서 SEC 등록 번호 및 인증서(CA) 번호를 받아야 합니다.
     - 또한 회사명, 업체명, PSEC 등록 번호, 금융/대출 기업 운영 인증서(CA)를 앱 설명에 공개해야 합니다.
   - P2P 대출이나 크라우드 펀딩 관련 규칙 및 규정(CF 규칙)에 정의된 바에 따른 대출 기반 크라우드 펀딩 활동에 참여하는 앱은 PSEC에 등록된 CF 중개인을 통해 거래를 처리해야 합니다.
4. **나이지리아**
   - 디지털 자금 대출 기관(DML)은 나이지리아 연방 경쟁 및 소비자 보호 위원회(FCCPC)의 2022년 디지털 대출에 관한 제한적 임시 규제/등록 프레임워크 및 가이드라인(때때로 개정될 수 있음)을 준수하고 완료해야 하며, FCCPC로부터 검증 가능한 승인서를 발급받아야 합니다.
   - 대출 애그리게이터는 디지털 대출 서비스에 관한 서류 및/또는 인증서 그리고 제휴를 맺은 모든 디지털 자금 대출 기관의 연락처 세부정보를 제공해야 합니다.
5. **케냐**
   - 디지털 신용 상품 제공업체(DCP)는 DCP 등록 프로세스를 완료하고 케냐 중앙 은행(CBK)의 라이선스를 획득해야 합니다. 선언 작성 시 CBK 라이선스의 사본을 제공해야 합니다.

- 대출 활동에 직접 참여하지는 않고 등록된 DCP로부터 사용자가 대출을 받도록 지원하는 플랫폼만 제공하는 경우 선언에 이를 정확하게 명시하고 관련 파트너의 DCP 라이선스 사본을 제공해야 합니다.
- 현재는 CBK 공식 웹사이트의 디지털 신용 상품 제공업체 디렉터리에 기재되어 있는 법인의 선언과 라이선스만 인정합니다.

6. **파키스탄**
   - 비은행 금융 기관(NBFC)에 속한 대출 기관은 기관마다 디지털 대출 앱(DLA)을 하나만 게시할 수 있습니다. NBFC당 둘 이상의 DLA를 게시하려고 시도하는 경우 개발자 계정 및 연결된 다른 계정이 폐쇄될 수 있습니다.
   - 파키스탄에서 디지털 대출 서비스를 제공 또는 알선하려면 SECP의 승인을 받은 증빙 서류를 제출해야 합니다.

7. **태국**
   - 태국을 타겟팅하며 금리가 15% 이상인 개인 대출 앱은 태국 은행(BoT) 또는 재무부(MoF)로부터 유효한 라이선스를 취득해야 합니다. 개발자는 태국에서 개인 대출을 제공하거나 알선할 능력을 입증하는 문서를 제공해야 합니다. 이 문서에는 다음이 포함되어야 합니다.
     - 개인 대출 제공업체 또는 소액 금융 조직으로 운영할 수 있도록 태국 은행에서 발행한 라이선스 사본
     - Pico 또는 Pico-plus 대출 제공업체로 운영할 수 있도록 재무부에서 발행한 Pico-finance 사업 허가증 사본

다음은 자주 발생하는 위반 사례입니다.



실제 현금 도박, 게임, 콘테스트

특정 요건을 충족하는 실제 현금 도박 앱, 실제 현금 도박 관련 광고, 게임화된 결과가 포함된 포인트 제도, 단기 판타지 스포츠 앱은 허용됩니다.

도박 앱

제한사항 및 모든 Google Play 정책 준수 여부에 따라 Google은 개발자가 Google Play에서 배포되는 도박 앱과 관련한 신청 절차를 완료 하고, 특정 국가에서 승인된 정부 사업자이거나 정부 도박 당국에 허가받은 사업자로 등

록되어 있으며, 제공하려는 온라인 도박 상품 유형에 관한 특정 국가 내 유효한 사업 허가증을 제시할 수 있는 경우 일부 국가에서 온라인 도박을 지원하거나 조장하는 앱을 허용합니다.

다음과 같은 유형의 온라인 도박 상품에 관한 유효한 허가 또는 승인을 받은 도박 앱만 허용됩니다.

- 온라인 카지노 게임
- 스포츠 베팅
- 경마(스포츠 베팅과 별도로 규제 및 허가되는 경우)
- 복권
- 단기 판타지 스포츠

자격을 갖춘 앱은 다음 요건을 충족해야 합니다.

- 개발자가 Google Play에 앱을 배포하려면 신청 절차를 완료해야 합니다.
- 앱이 배포되는 각 국가에 적용되는 모든 관련 법규 및 업계 표준을 준수해야 합니다.
- 개발자는 앱이 배포되는 각 국가 또는 주/준주에서 유효한 도박 허가를 받아야 합니다.
- 개발자는 도박 허가의 범위를 벗어나는 도박 상품 유형을 제공해서는 안 됩니다.
- 미성년 사용자가 앱을 사용하지 못하도록 제한해야 합니다.
- 개발자가 제시한 도박 허가증이 적용되지 않는 국가, 주/준주 또는 지역에서 앱을 사용할 수 없어야 합니다.
- Google Play에 유료 앱으로 등록하거나 Google Play 인앱 결제를 사용해서는 안 됩니다.
- Google Play 스토어에서 앱을 무료로 다운로드하고 설치할 수 있어야 합니다.
- 성인 전용(AO) 또는 이에 해당하는 IARC 등급이 부여된 앱이어야 합니다.
- 앱과 앱 등록정보에 책임감 있는 도박 문화에 관한 정보가 명시되어 있어야 합니다.

기타 실제 현금 게임, 콘테스트 및 토너먼트 앱

위에 명시된 도박 앱 자격요건을 충족하지 않으며 아래 명시된 '기타 실제 현금 게임 파일럿'에 포함되지 않는 기타 모든 앱의 경우, 사용자가 실제 금전적 가치가 있는 상품을 획득하기 위해 실제 현금(현금으로 구매한 인앱 상품 포함)으로 내기를 하거나 돈을 걸거나 이에 참여하도록 지원하거나 조장하는 콘텐츠 또는 서비스는 허용되지 않습니다. 여기에는 온라인 카지노, 스포츠 베팅, 복권, 돈을 받고 현금 또는 기타 실물 가치를 상품으로 제공하는 게임이 포함되나 이에 국한되지 않습니다(아래에 설명된 게임화된 포인트 제도 요건에서 허용하는 프로그램 제외).

위반 사례

- 실물 또는 금전적 부상을 획득할 기회의 대가로 돈을 받는 게임
- 메뉴 항목, 탭, 버튼, WebView 등의 탐색 요소를 통해 실제 현금으로 내기를 하거나 돈을 걸거나 실제 현금 게임, 콘테스트, 토너먼트에 참여하도록 '클릭 유도문안'을 제공하는 앱(예: 현금 부상의 기회를 위한 토너먼트에 '베팅'하거나 '등록'하거나 '경쟁'하도록 사용자를 독려함).
- 내기, 인앱 화폐, 상금 또는 도박을 하거나 실물/금전적 부상을 획득하기 위한 송금을 수락하거나 관리하는 앱

기타 실제 현금 게임 파일럿

일부 지역에서 때에 따라 특정 유형의 실제 현금 게임 파일럿을 한정된 기간 동안 진행할 수 있습니다. 자세한 내용은 고객센터 페이지를 참고하세요. 일본 내 온라인 인형 뽑기 게임 파일럿은 2023년 7월 11일에 종료됩니다. 2023년 7월 12일부터 온라인 인형 뽑기 게임 앱은 특정 요건 및 관련 법률을 충족하면 전 세계의 Google Play에 등록될 수 있습니다.

게임 요소가 포함된 포인트 제도

법률에 의해 허용되며 도박 또는 게임에 대한 추가적 라이선스 요구사항이 적용되지 않는 경우에 한해, 다음과 같은 Play 스토어 자격요건을 준수하는 조건으로 사용자에게 실물 상품 또는 이에 상응하는 금전적 상품을 제공하는 포인트 제도가 허용됩니다.

모든 앱(게임 및 비게임):

- 포인트 제도의 혜택이나 리워드는 앱 내에서 조건을 충족하는 금전 거래에 대해 명확하게 보완적이고 부차적(즉 해당 금전 거래는 포인트 제도와는 별개의 상품 또는 서비스를 제공하기 위한 완전히 별도의 거래여야 함)이어야

합니다. 또한 혜택이나 리워드는 구매 가능하거나 어떠한 교환 유형과도 연결되어서는 안 되며, 그렇지 않으면 '실제 현금 도박, 게임, 콘테스트' 정책 제한사항 위반에 해당합니다.

- 예를 들어 조건을 충족하는 금전 거래의 어떤 부분도 포인트 제도에 참여하기 위한 수수료나 내기 금액에 해당해서는 안 되며, 해당 금전 거래로 인해 정상가를 초과하는 금액으로 상품이나 서비스를 구매하게 되어서는 안 됩니다.

게임 앱:

- 적립 포인트 또는 혜택이 제공되는 리워드, 특전 또는 조건을 충족하는 금전 거래와 관련된 리워드는 고정 비율을 기준으로만 제공 및 사용해야 합니다. 이 경우 해당 비율을 포인트 제도의 공식적인 규정이 게재된 위치 및 앱에서 눈에 잘 띄는 위치에 명시해야 하며, 게임 실적 또는 운에 따른 결과에 따라 적립 포인트 또는 리워드를 베팅, 제공 또는 증가할 수 있게 해서는 **안 됩니다**.

비게임 앱:

- 적립 포인트나 리워드는 아래에 명시된 요건을 충족할 경우 콘테스트 또는 운에 따른 결과와 연관될 수 있습니다. 조건을 충족하는 금전 거래와 연결된 혜택 또는 리워드를 제공하는 포인트 제도는 다음 요건을 충족해야 합니다.
  - 앱 내에 포인트 제도의 공식 규정을 게시해야 합니다.
  - 가변적이거나 운에 따르거나 무작위로 보상을 제공하는 시스템을 포함하는 포인트 제도의 경우 공식 약관에 1) 보상을 결정하는 고정 확률을 사용하는 포인트 제도의 확률, 2) 그러한 기타 포인트 제도에서 사용하는 선정 방법(예: 보상을 결정하는 데 사용되는 변수)을 공개해야 합니다.
  - 추첨, 복권 또는 기타 유사한 스타일의 프로모션을 제공하는 포인트 제도의 공식 약관에 프로모션마다 고정된 우승자 수, 고정된 참가 마감일, 상품 제공일을 지정해야 합니다.
  - 적립 포인트 또는 리워드가 고정 비율로 누적 및 사용된다면 앱 내에서 눈에 잘 띄는 위치 및 포인트 제도의 공식 약관 내에 해당 비율을 명시해야 합니다.

포인트 제도를 제공하는 앱의 유형	게임 요소가 포함된 포인트 제도 및 변동적 리워드	고정 비율/일정에 따른 포인트 리워드	포인트 제도 이용약관 필요	이용약관에 운에 따르는 포인트 제도의 확률 또는 선정 방법을 공개해야 함
게임	허용되지 않음	허용	필수	해당 사항 없음(게임 앱의 포인트 제도에는 운에 따르는 요소가 포함될 수 없음)
비게임	허용	허용	필수	필수

Play에서 배포되는 앱 내의 도박 또는 실제 현금 게임, 콘테스트, 토너먼트에 관한 광고

다음 요건을 충족하는 경우 도박, 실제 현금 게임, 콘테스트, 토너먼트를 홍보하는 광고가 포함된 앱이 허용됩니다.

- 앱과 광고(광고주 포함)는 광고가 게재되는 지역에 적용되는 모든 관련 법규 및 업계 표준을 준수해야 합니다.
- 홍보하는 모든 도박 관련 상품 및 서비스에 적용되는 모든 관련 현지 광고 허가 요건을 광고가 충족해야 합니다.
- 만 18세 미만으로 확인된 개인은 앱에서 도박 광고를 볼 수 없어야 합니다.
- 앱이 가족을 위한 앱 프로그램에 등록되어 있지 않아야 합니다.
- 앱이 만 18세 미만의 개인을 타겟팅하지 않아야 합니다.
- 위에 정의된 바에 따른 도박 앱을 광고하는 경우 앱의 방문 페이지, 광고되는 앱의 등록정보나 앱 내에 책임감 있는 도박 문화에 관한 정보가 명확히 게재되어 있어야 합니다.
- 앱에서 시뮬레이션 도박 콘텐츠(예: 소셜 카지노 앱, 가상 슬롯머신이 포함된 앱)를 제공해서는 안 됩니다.
- 앱에서 도박 또는 실제 현금 게임, 복권, 토너먼트 지원/컴패니언 기능(예: 내기, 지불, 스포츠 경기 결과/배당률/실적 추적 또는 참여 자금 관리 등을 지원하는 기능)을 제공해서는 안 됩니다.
- 앱 콘텐츠는 사용자에게 도박 또는 실제 현금 게임, 복권, 토너먼트 서비스를 홍보하거나 안내해서는 안 됩니다.

위 섹션에 명시된 모든 요건을 충족하는 앱에만 도박 또는 실제 현금 게임, 복권, 토너먼트 광고가 포함될 수 있습니다. 위의 1~6번 요건을 충족하는 승인된 도박 앱(위의 정의에 따름) 또는 승인된 단기 판타지 스포츠 앱(아래 정의에 따름)에만 도박 또는 실제 현금 게임, 복권, 토너먼트 광고가 포함될 수 있습니다.

위반 사례

- 미성년 사용자를 대상으로 하면서 도박 서비스를 홍보하는 광고가 표시되는 앱
- 사용자에게 실제 현금 카지노를 홍보하거나 안내하는 시뮬레이션 카지노 게임
- 스포츠 베팅 사이트로 연결되는 도박 광고가 통합된 전용 스포츠 배당률 추적 앱
- 사용자에게 버튼, 아이콘 또는 기타 대화형 인앱 요소로 표시되는 광고와 같이 Google의 사기성 광고 정책을 위반하는 도박 광고가 포함된 앱

단기 판타지 스포츠(DFS) 앱

해당하는 현지 법규에 따라 정의된 단기 판타지 스포츠(DFS) 앱은 다음 요건을 충족하는 경우에만 허용됩니다.

- 앱은 1) 미국 내에서만 배포되거나 2) 미국 외 국가의 경우 위에 언급된 도박 앱 요건 및 신청 절차를 충족해야 합니다.
- 개발자가 Play에 앱을 배포하려면 DFS 신청 절차를 완료하고 수락되어야 합니다.
- 앱은 배포되는 국가의 모든 관련 법규와 업계 표준을 준수해야 합니다.
- 미성년 사용자가 앱 내에서 도박이나 금전 거래를 하지 못하도록 제한해야 합니다.
- Google Play에 유료 앱으로 등록하거나 Google Play 인앱 결제를 제공해서는 안 됩니다.
- 스토어에서 앱을 무료로 다운로드하고 설치할 수 있어야 합니다.
- 성인 전용(AO) 또는 이에 해당하는 IARC 등급이 부여된 앱이어야 합니다.
- 앱과 앱 등록정보에 책임감 있는 도박 문화에 관한 정보가 명시되어 있어야 합니다.
- 앱이 배포되는 미국 주 또는 준주에 적용되는 모든 관련법 및 업계 표준을 준수해야 합니다.
- 개발자는 단기 판타지 스포츠 앱에 허가가 필요한 모든 미국 주 또는 준주에서 유효한 허가를 갖고 있어야 합니다.
- 개발자가 단기 판타지 스포츠 앱에 필요한 허가를 갖고 있지 않은 미국 주 또는 준주에서 앱을 사용할 수 없어야 합니다.
- 단기 판타지 스포츠 앱이 합법이 아닌 미국 주 또는 준주에서 앱을 사용할 수 없어야 합니다.

불법 활동

불법 활동을 지원하거나 조장하는 앱은 허용되지 않습니다.

다음은 자주 발생하는 위반 사례입니다.

- 불법 약물을 판매 또는 구매하도록 조장합니다.
- 미성년자의 마약, 주류, 담배 사용 또는 판매를 묘사하거나 조장합니다.
- 불법 약물의 재배 또는 제조 방법을 안내합니다.

사용자 제작 콘텐츠

사용자 제작 콘텐츠(UGC)는 사용자가 제작하여 앱에 제공하는 콘텐츠로, 일부 또는 전체 앱 사용자가 보거나 액세스할 수 있습니다.

사용자를 UGC 플랫폼으로 안내하는 전용 브라우저/클라이언트를 비롯해 UGC를 포함하거나 제공하는 앱은 다음과 같이 강력하고 효과적이며 지속적인 UGC 검토를 시행해야 합니다.

- 사용자가 UGC를 제작하거나 업로드하기 전에 앱의 이용약관 및/또는 사용자 정책을 수락하도록 해야 합니다.
- Google Play 개발자 프로그램 정책을 준수하는 방식으로 불쾌감을 주는 콘텐츠와 행동을 규정하고, 앱의 이용약관 또는 사용자 정책을 통해 해당 콘텐츠와 행동을 금지해야 합니다.
- 앱을 통해 호스팅되는 UGC의 유형에 부합하는 합리적인 방식으로 UGC 검토를 진행합니다. 여기에는 불쾌감을 주는 UGC 및 사용자를 신고 및 차단하고 적절한 경우 UGC나 사용자에 대한 조치를 취하기 위한 인앱 시스템이 포함됩니다. 각각의 UGC 경험에 따라 검토의 유형이 달라질 수 있습니다. 예를 들면 다음과 같습니다.
  - 사용자 확인 또는 오프라인 등록(예: 특정 학교나 기업 내에서만 사용되는 앱)과 같은 수단을 통해 특정 사용자를 식별할 수 있는 UGC 앱은 반드시 콘텐츠 및 사용자를 신고할 수 있는 인앱 기능을 제공해야 합니다.

- 특정 사용자와의 1:1 상호작용을 제공하는 UGC 기능(예: 채팅 메시지, 태그, 멘션 등)은 반드시 사용자를 차단하는 인앱 기능을 제공해야 합니다.
- 소셜 네트워킹 앱이나 블로그 앱과 같이 공개적으로 액세스할 수 있는 UGC에 대한 액세스를 제공하는 앱은 반드시 사용자 및 콘텐츠 신고와 사용자 차단을 위한 인앱 기능을 구현해야 합니다.
- 증강 현실(AR) 앱의 경우 UGC 검토(앱 내 신고 시스템 포함) 시 불쾌감을 주는 AR UGC(예: 외설적인 AR 이미지)와 민감한 AR 앵커링 위치(예: 군사 기지 또는 AR 앵커링으로 인해 소유자에게 문제가 발생할 수 있는 사유지 등 제한된 지역에 앵커링된 AR 콘텐츠)를 모두 고려해야 합니다.

- 불쾌감을 주는 사용자 행동을 조장하여 인앱 수익을 창출하는 행위를 방지하기 위한 보호 장치를 제공해야 합니다.

부수적인 성적 콘텐츠

(1) 주로 성적이지 않은 콘텐츠에 대한 액세스를 제공하며 (2) 성적인 콘텐츠를 적극적으로 홍보하거나 추천하지 않는 UGC 앱에 표시되는 성적인 콘텐츠는 '부수적인' 것으로 간주됩니다. 관련 법에서 불법으로 정의하는 성적인 콘텐츠와 아동 학대 콘텐츠는 '부수적인' 것으로 간주되지 않으며 허용되지도 않습니다.

UGC 앱은 다음의 요건이 모두 충족되는 경우에만 부수적인 성적 콘텐츠를 포함할 수 있습니다.

- 해당 콘텐츠가 최소 2가지의 사용자 작업을 거쳐야 완전히 사용 중지할 수 있는 필터 뒤에 기본적으로 숨겨져 있어야 합니다(예: 표시 차단 필터 뒤에 배치되어 있거나 '세이프서치'를 사용 중지하지 않으면 기본적으로 볼 수 없는 콘텐츠).
- 가족 정책에 정의된 아동이 연령 심사 시스템(중립적인 연령 심사나 관련 법에 정의된 적절한 시스템)을 사용하여 앱에 액세스하는 것이 명시적으로 금지되어 있어야 합니다.
- 앱이 콘텐츠 등급 정책에 따라 UGC와 관련된 콘텐츠 등급 설문지에 정확하게 응답해야 합니다.

불쾌감을 주는 UGC를 제공하는 것이 주 목적인 앱은 Google Play에서 삭제됩니다. 마찬가지로 불쾌감을 주는 UGC를 호스팅하는 데 주로 사용되거나 사용자 사이에서 이러한 콘텐츠가 활발하게 공유되는 공간으로 알려진 앱도 Google Play에서 삭제됩니다.

다음은 자주 발생하는 위반 사례입니다.

- 주로 불쾌감을 주는 콘텐츠의 공유를 조장하는 유료 기능을 구현하거나 허용하는 등 선정적인 사용자 제작 콘텐츠를 홍보합니다.
- 미성년자를 대상으로 하며 위협, 괴롭힘 또는 폭력을 방지하는 충분한 보호 장치가 마련되지 않은 사용자 제작 콘텐츠(UGC)가 앱에 포함되어 있습니다.
- 학대, 악의적인 공격 또는 조롱할 목적으로 다른 사람을 괴롭히거나 따돌리려는 의도가 담긴 게시물, 댓글 또는 사진이 앱에 포함되어 있습니다.
- 불쾌감을 주는 콘텐츠에 관한 사용자 불만을 앱에서 해결하지 못하는 상황이 계속됩니다.

건강 관련 콘텐츠 및 서비스

유해한 건강 관련 콘텐츠 및 서비스에 사용자를 노출하는 앱은 허용되지 않습니다.

앱에 건강 관련 콘텐츠 및 서비스가 포함되어 있거나 이를 홍보하는 경우 관련된 모든 법률 및 규정을 준수해야 합니다.

건강 앱

앱이 건강 데이터에 액세스하고 건강 앱이거나 건강 관련 기능을 제공하는 경우 아래 요구사항 외에 개인 정보 보호, 사기 및 악용, 민감한 사건 등 기존 Google Play 개발자 정책도 준수해야 합니다.

- **Console 선언:**
  - Play Console에서 앱 콘텐츠 페이지(정책 > 앱 콘텐츠)로 이동한 다음 앱이 속한 카테고리를 선택하세요.
- **개인정보처리방침 및 명시적 공개 요건:**
  - 앱은 Play Console의 지정된 필드에 개인정보처리방침 링크를, 앱 자체에는 개인정보처리방침 링크 또는 텍스트를 게시해야 합니다. 개인정보처리방침이 PDF가 아니고 공개적으로 액세스 가능하고 지오펜싱되지 않은 URL을 통해 실제로 접속할 수 있으며 수정 불가능한지 확인하시기 바랍니다(데이터 보안 섹션에 따름).

- 모든 인앱 공개와 더불어 앱의 개인정보처리방침에서는 개인 또는 민감한 사용자 데이터의 액세스, 수집, 사용, 공유를 포괄적으로 공개해야 하며, 이는 위의 데이터 보안 섹션에 공개된 데이터로 국한되지 않습니다. 기능 또는 데이터가 위험한 권한 또는 런타임 권한 에 의해 규제되는 경우 앱은 모든 관련 명시적 공개 및 동의 요건을 이행해야 합니다.
- 건강 앱이 핵심 기능을 수행하는 데 필요하지 않은 권한을 요청해서는 안 되며, 사용되지 않는 권한은 삭제해야 합니다. 건강 관련 민감한 정보의 범위에 포함되는 권한 목록은 건강 앱 카테고리 및 추가 정보를 참고하세요.
- 앱이 기본적으로 건강 앱은 아니지만 건강 관련 기능이 있고 건강 데이터에 액세스하는 경우에도 건강 앱 정책의 범위에 포함됩니다. 앱의 핵심 기능과 건강 관련 데이터의 수집 간 연관성을 사용자가 명확히 이해할 수 있어야 합니다. 보험 제공업체, 게임 플레이를 진행하는 방식으로 사용자의 활동 데이터를 수집하는 게임 앱 등을 예로 들 수 있습니다. 앱의 개인정보처리방침에 이러한 용도 제한이 명시되어야 합니다.

- **추가 요구사항:**
  건강 앱이 다음 지정 중 하나에 해당하는 경우 Play Console에서 적절한 카테고리를 선택하는 것 외에 관련 요구사항도 준수해야 합니다.
  - **정부 제휴 건강 앱:** 정부 또는 공인 의료 기관에서 제휴를 통해 공인 앱을 개발하고 배포할 권한을 부여받은 경우 사전 알림 양식을 통해 자격 요건 증빙을 제출해야 합니다.
  - **접촉자 추적/건강 상태 앱:** 앱이 접촉자 추적 및/또는 건강 상태 앱인 경우 Play Console에서 '질병 예방 및 공공 보건'을 선택한 다음 위의 사전 알림 양식을 통해 필요한 정보를 제공하세요.
  - **인간 대상 연구 앱:** 건강과 관련해 인간을 대상으로 연구를 수행하는 앱은 모든 규칙과 규정을 따라야 하며, 참여자 또는 부모나 보호자(참여자가 미성년자인 경우)에게 충분한 설명에 기반한 동의를 구할 의무를 포함하되 이에 국한되지 않습니다. 건강 연구 앱은 달리 면제되지 않는 한 기관의 검토 위원회(IRB) 및/또는 상응하는 독립 윤리 위원회의 승인을 받아야 합니다. 요청 시 그러한 승인의 증빙이 제공되어야 합니다.
  - **의료 기기 또는 SaMD 앱:** 의료 기기 또는 SaMD로 간주되는 앱은 규제 기관이나 건강 앱의 거버넌스 및 규정 준수를 담당하는 기구에서 제공한 허가서 또는 승인 문서를 획득하여 보유해야 합니다. 요청 시 그러한 허가 또는 승인의 증빙이 제공되어야 합니다.

헬스 커넥트 데이터

헬스 커넥트 권한을 통해 액세스되는 데이터는 사용자 데이터 정책이 적용되는 개인 정보 및 민감한 사용자 데이터로 간주되며, 여기에는 추가 요건 이 적용됩니다.

처방의약품

처방 없이 처방의약품을 판매하거나 구매하기 용이하게 하는 앱은 허용되지 않습니다.

승인되지 않은 약물

Google Play에서는 승인되지 않은 약물을 홍보하거나 판매하는 앱을 허용하지 않으며, 이는 판매자가 주장하는 합법성과 무관합니다.

다음은 자주 발생하는 위반 사례입니다.

- 금지된 의약품 및 건강보조식품 목록(해당하는 제품이 목록에 모두 포함된 것은 아님)에 있는 모든 제품
- 에페드라 함유 제품
- 체중 감량/체중 조절, 단백동화 스테로이드와 연관 지어 홍보하는 hCG(인간 융모성 생식선 자극호르몬) 함유 제품
- 원료 의약품 또는 위험한 성분이 함유된 약초 보조제 및 건강보조식품
- 처방약 또는 규제 약물과 동일한 효과가 있음을 암시하는 주장 등 건강에 관한 허위 주장이나 오해의 소지가 있는 주장을 하는 제품
- 정부의 승인을 받지 않은 제품을 특정 질병/질환 예방 또는 치료에 안전하거나 효과적이라고 홍보하는 제품
- 정부나 관련 기관의 조치 또는 경고를 받은 제품
- 승인되지 않은 의약품, 건강보조식품, 규제 약물과 이름이 유사하여 혼동할 수 있는 제품

Google에서 모니터링하는 의약품 및 건강보조식품 중 승인되지 않았거나 소비자에게 왜곡된 정보를 제공하는 제품에 관해 자세히 알아보려면 www.legitscript.com 사이트를 참고하세요.

잘못된 건강 관련 정보

기존의 의학적 통설과 상충하거나 사용자에게 해를 입힐 수 있는 잘못된 보건 관련 주장을 포함하는 앱은 허용되지 않습니다.

다음은 자주 발생하는 위반 사례입니다.

- 백신이 DNA를 변형시킬 수 있다는 등 백신에 관한 왜곡된 주장
- 유해하고 승인되지 않은 치료법의 옹호
- 성적 지향 전환 치료 등 기타 유해한 건강 관련 관행의 옹호

의료 기능

오해를 일으키거나 해를 입힐 수 있는 의료 또는 건강 관련 기능이 있는 앱은 허용되지 않습니다. 예를 들어 앱만 사용하여 산소 포화도 측정 기능을 제공한다고 주장하는 앱은 허용되지 않습니다. 산소 포화도 측정기 앱은 산소 포화도 측정 기능이 있는 외부 하드웨어, 웨어러블 또는 전용 스마트폰 센서의 지원이 있어야 합니다. 지원을 받는 앱 역시 의료용이 아니며 일반적인 피트니스 및 건강 관리 목적으로만 사용해야 하고 의료 기기가 아니라는 사실이 명시된 면책조항을 메타데이터에 포함해야 하며, 호환되는 하드웨어 모델/기기 모델을 정확하게 공개해야 합니다.

결제 - 임상 서비스

규제 대상 임상 서비스와 관련된 거래에 Google Play 결제 시스템을 사용해서는 안 됩니다. 자세한 내용은 Google Play 결제 정책 이해 를 참고하세요.

블록체인 기반 콘텐츠

블록체인 기술이 계속해서 빠르게 발전함에 따라 Google에서는 개발자가 혁신 기술을 통해 성공을 거두고 더 풍부하면서 몰입감 있는 사용자 환경을 구축할 수 있는 플랫폼을 제공하는 것을 목표하고 있습니다.

이 정책에서 블록체인 기반 콘텐츠란 블록체인에서 확보한 토큰화된 디지털 애셋을 의미합니다. 앱에 블록체인 기반 콘텐츠가 포함되는 경우 이러한 요건을 준수해야 합니다.

암호화폐 거래소 및 소프트웨어 지갑

암호화폐의 구매, 소유 또는 교환은 규제 대상 관할권 내 인증받은 서비스를 통해 이루어져야 합니다.

또한 앱이 타겟팅하는 모든 지역 또는 국가의 관련 규정을 준수해야 하며, 제품 및 서비스가 금지된 곳에서 앱을 게시해서는 안 됩니다. Google Play에서는 관련 규제 또는 라이선스 요건 준수와 관련하여 추가 정보 또는 문서를 제공하도록 요청할 수 있습니다.

암호화폐 채굴

기기에서 암호화폐를 채굴하는 앱은 허용되지 않습니다. 암호화폐 채굴을 원격 관리하는 앱은 허용됩니다.

토큰화된 디지털 애셋 배포에 관한 투명성 요건

앱에서 토큰화된 디지털 애셋을 판매하거나 사용자가 이를 획득할 수 있도록 하는 경우, Play Console의 '앱 콘텐츠' 페이지에 있는 금융 기능 선언 양식을 통해 이 사실을 선언해야 합니다.

인앱 상품을 만드는 경우 토큰화된 디지털 애셋을 제공한다는 사실을 제품 세부정보에 명시해야 합니다. 추가 안내는 인앱 상품 만들기를 참고하세요.

플레이 또는 거래 활동으로부터 얻을 수 있는 잠재적 수익을 홍보하거나 미화할 수 없습니다.

NFT 게임화에 대한 추가 요건

Google Play의 실제 현금 도박, 게임, 콘테스트 정책에 따라 NFT와 같이 토큰화된 디지털 애셋을 통합하는 도박 앱은 신청 절차를 완료해야 합니다.

도박 앱 자격요건을 충족하지 않으며 기타 실제 현금 게임 파일럿에 포함되지 않는 기타 모든 앱의 경우, 가치가 알려지지 않은 NFT를 획득할 기회를 얻는 대가로 금전적 가치가 있는 어떠한 것도 받아서는 안 됩니다. 사용자가 구매한 NFT는 사용자 경험을 개선하거나 사용자가 게임을 진행하는 데 도움을 받기 위해 게임 내에서 소비 또는 사용되어야 합니다. 실제 금전적 가치가 있는 상품(다른 NFT 포함)을 획득할 기회를 얻는 대가로 내기를 하거나 돈을 거는 데 NFT를 사용해서는 안 됩니다.

다음은 자주 발생하는 위반 사례입니다.

- NFT의 구체적인 콘텐츠 및 가치를 공개하지 않고 NFT 번들을 판매하는 앱
- NFT를 리워드로 제공하는 유료 플레이 소셜 카지노 게임(예: 슬롯 머신)

AI 생성 콘텐츠

개발자 사이에서 생성형 AI 모델이 점점 더 폭넓게 사용됨에 따라, 사용자 참여도를 높이고 사용자 환경을 개선하기 위하여 생성형 AI 모델을 앱에 통합하는 개발자도 있을 것입니다. Google Play는 AI 생성 콘텐츠가 모든 사용자에게 안전할 뿐만 아니라 사용자 의견 반영을 통해 책임감 있는 혁신이 이루어질 수 있도록 지원하고자 합니다.

AI 생성 콘텐츠

AI 생성 콘텐츠는 사용자 프롬프트를 기반으로 생성형 AI 모델이 생성한 콘텐츠입니다. AI 생성 콘텐츠의 예시는 다음과 같습니다.

- 챗봇과의 상호작용이 앱의 주요 기능인 텍스트 기반 대화 생성형 AI 챗봇
- 텍스트, 이미지, 음성 프롬프트에 따라 AI에 의해 생성된 이미지

사용자의 안전을 보증하고 Google Play의 정책 범위를 준수하기 위하여 AI를 사용해 콘텐츠를 생성하는 앱은 반드시 기존의 Google Play 개발자 정책을 준수해야 합니다. 여기에는 아동 착취 또는 학대를 조장하는 콘텐츠 및 사기성 행위에 사용되는 콘텐츠 등의 제한된 콘텐츠 생성 금지 및 예방이 포함됩니다.

AI를 사용해 콘텐츠를 생성하는 앱은 반드시 앱 내에 사용자 보고 또는 신고 기능을 갖추고 있어야 하며, 사용자가 앱을 종료하지 않고도 이러한 기능을 사용해 불쾌감을 주는 콘텐츠를 개발자에게 신고할 수 있어야 합니다. 또한 개발자는 사용자 신고를 활용하여 앱 내에 콘텐츠 필터링 및 검토 조치를 취해야 합니다.

지적 재산권

앱 또는 개발자 계정으로 상표권, 저작권, 특허권, 영업비밀, 기타 독점적 권리 등 다른 사람의 지적 재산권을 침해해서는 안 됩니다. 앱을 통해 다른 사람의 지적 재산권을 침해하도록 조장 또는 유도해서도 안 됩니다.

Google은 저작권 침해가 의심되는 사항에 대한 명확한 신고가 있을 경우 이에 대응합니다. 자세한 내용을 보거나 DMCA에 따라 이의신청을 하려면 Google의 저작권 절차 를 참조하시기 바랍니다.

앱 내의 모조품 판매 또는 홍보와 관련한 위반사항을 신고하려면 모조품 신고 양식을 제출해 주세요.

상표 소유자로서 Google Play에 내 상표권을 침해하는 앱이 있다고 생각되는 경우 개발자에게 직접 연락하여 문제를 해결하시기 바랍니다. 개발자의 도움으로도 문제를 해결할 수 없다면 이 양식 을 통해 상표권 침해 신고를 제출해 주세요.

앱 또는 스토어 등록정보에 제3자의 지적 재산권(예: 브랜드 이름 및 로고, 그래픽 저작물 등)을 사용할 권리를 증명하는 서류가 있는 경우, 앱을 제출하기 전에 Google Play팀에 문의 하여 앱이 지적 재산권 침해로 거부되지 않도록 하세요.

저작권 보호를 받는 콘텐츠 무단 사용

저작권을 침해하는 앱은 허용되지 않습니다. 저작권 보호 콘텐츠를 수정하시는 경우에도 정책 위반으로 간주될 수 있습니다. 개발자가 저작권 보호 콘텐츠를 사용하려면 권한을 입증해야 할 수도 있습니다.

앱의 기능을 보여주기 위해 저작권 보호를 받는 콘텐츠를 사용할 때 주의하시기 바랍니다. 일반적으로 가장 안전한 방법은 독창적인 콘텐츠를 만드는 것입니다.

다음은 자주 발생하는 위반 사례입니다.

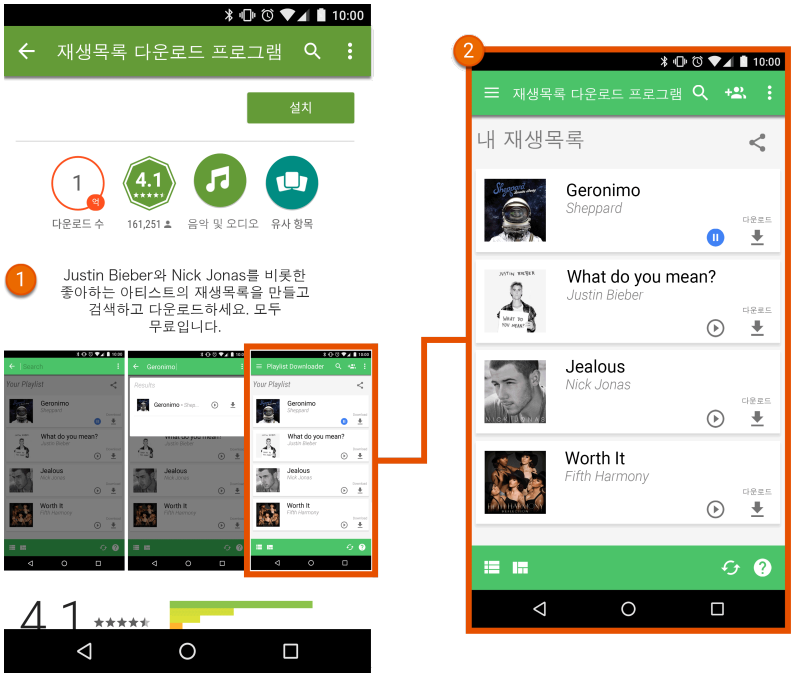
- 음악 앨범, 비디오 게임, 책의 커버 이미지입니다.
- 영화, TV 프로그램, 비디오 게임의 마케팅 이미지입니다.
- 만화책, 만화, 영화, 뮤직비디오, TV 프로그램의 포스터 또는 이미지입니다.
- 대학 및 프로 스포츠 팀 로고입니다.
- 유명 인사의 소셜 미디어 계정에서 가져온 사진입니다.
- 유명 인사를 전문 사진사가 촬영한 이미지입니다.
- 저작권 보호를 받는 원본과 구별할 수 없는 복제물 즉, '팬아트'입니다.
- 앱이 저작권 보호를 받는 콘텐츠의 오디오 클립을 재생하는 사운드보드를 포함합니다.
- 공개 도메인에 없는 책의 전체 복제물 또는 번역물입니다.

저작권을 침해하도록 조장

앱이 다른 사람의 저작권을 침해하도록 조장 또는 유도해서는 안 됩니다. 앱을 게시하기 전에 저작권 침해를 조장할 우려가 있는지 확인하고 필요한 경우 법률 자문을 받아야 합니다.

다음은 자주 발생하는 위반 사례입니다.

- 저작권 보호를 받는 콘텐츠의 로컬 사본을 허가 없이 다운로드하도록 허용하는 스트리밍 앱입니다.
- 관련 저작권법을 위반하며 음악, 동영상 등의 저작권 보호를 받는 저작물을 스트리밍 또는 다운로드하도록 조장하는 앱입니다.



① 이 앱 등록정보의 설명은 저작권 보호를 받는 콘텐츠를 허가 없이 다운로드하도록 조장합니다.
② 이 앱 등록정보의 스크린샷은 저작권 보호를 받는 콘텐츠를 허가 없이 다운로드하도록 조장합니다.

상표권 침해

다른 사람의 상표권을 침해하는 앱은 허용되지 않습니다. 상표는 상품 또는 서비스의 원천을 식별하는 단어나 기호 또는 둘의 조합입니다. 상표권을 획득한 후에는 소유자에게 특정 상품 또는 서비스와 관련하여 상표 사용에 대한 독점권이 부여됩니다.

상표권 침해는 해당 상품의 원천을 혼동시키는 방식으로 동일하거나 유사한 상표를 부적절하거나 무단으로 사용하는 것을 말합니다. 다른 사람의 상표권을 사용하여 사용자 혼란을 일으킬 수 있는 경우 앱이 정지될 수 있습니다.

모조품

모조품을 판매하거나 홍보하는 앱은 허용되지 않습니다. 모조품에는 진품과 동일하거나 구분이 힘들 정도로 비슷한 상표권 또는 로고가 사용됩니다. 위조업자는 제품의 브랜드 표시를 모방하여 모조품을 해당 브랜드 소유권자의 진품으로 위장합니다.

개인정보 보호, 사기 및 기기 악용

Google에서는 사용자 개인정보를 보호하고 사용자 환경을 안전하게 유지하기 위해 노력하고 있습니다. 사기성 앱, 악성 앱 또는 네트워크, 기기, 개인 정보를 악용 또는 오용하기 위한 앱은 엄격하게 차단됩니다.

사용자 데이터

사용자 데이터(예: 기기 정보를 포함하여 사용자로부터 수집하거나 사용자에 관해 수집한 정보)를 투명하게 처리해야 합니다. 이는 앱 사용자 데이터의 액세스, 수집, 사용, 처리, 공유에 관해 공개하고 데이터의 용도를 공개된 정책 준수 목적으로 제한한다는 의미입니다. 또한 개인 정보 및 민감한 사용자 데이터의 처리에는 아래의 '개인 정보 및 민감한 사용자 데이터' 섹션에 명시된 추가 요건도 적용됩니다. 본 정책과 기타 Play 개발자 프로그램 정책 외에도 귀하는 항상 귀하의 제품 또는 서비스가 제공되는 관할에서의 개인 정보 보호 및 데이터 보호 법령을 준수해야 합니다. 예를 들어, 귀하가 유럽연합의 사용자에게 서비스를 제공하는 경우 프랑스 데이터 보호 당국(CNIL)에서 모바일 환경 내 개인 정보 보호에 관한 권장사항 가이드 를 채택하고 있으므로 이를 참고하면 도움이 될 수 있습니다.

앱에 SDK와 같은 서드 파티 코드가 포함되는 경우 앱에 사용된 서드 파티 코드와 앱의 사용자 데이터와 관련된 해당 서드 파티의 관행이 Google Play 개발자 프로그램 정책을 준수하는지 확인해야 하며, 여기에는 사용 및 공개 요건이 포함됩니다. 예를 들어 SDK 제공업체가 앱의 개인 정보 및 민감한 사용자 데이터를 판매하지 않는지 확인해야 합니다. 이 요건은 사용자 데이터가 서버로 전송된 후 이전되는지 또는 앱에 서드 파티 코드를 삽입하는 방식인지 여부와 관계없이 적용됩니다.

개인 정보 및 민감한 사용자 데이터

개인 정보와 민감한 사용자 데이터에는 개인 식별 정보, 금융 및 결제 정보, 인증 정보, 연락처 목록, 연락처, 기기 위치 , SMS 및 통화 관련 데이터, 건강 데이터 , 헬스 커넥트 데이터, 기기에 있는 다른 앱, 마이크, 카메라의 목록, 기타 민감한 기기 또는 사용 데이터가 포함되지만 이에 국한되지 않습니다. 앱에서 개인 정보와 민감한 사용자 데이터를 처리하는 경우 다음을 준수해야 합니다.

- 앱을 통해 획득한 개인 정보 및 민감한 사용자 데이터의 액세스, 수집, 사용, 공유는 사용자가 합리적으로 예상하는 앱 및 서비스 기능과 정책에 부합하는 목적으로 제한됩니다.
  - 광고 게재를 위해 개인 정보 및 민감한 사용자 데이터의 사용을 확장하는 앱은 Google Play의 광고 정책 을 준수해야 합니다.
  - 서비스 제공업체 의 필요에 따라 또는 유효한 정부 요청이나 관련 법률의 준수와 같이 법적인 사유, 합병 또는 인수의 일환으로 사용자에게 적절하게 합법적인 공지를 한 경우에도 데이터를 전송할 수 있습니다.
- 전송에 최신 암호화 기술(예: HTTPS 연결)을 사용하는 등 모든 개인 정보 및 민감한 사용자 데이터를 안전하게 처리합니다.
- 가능한 경우 Android 권한 을 통해 관리되는 데이터에 액세스하기 전에 런타임 권한 요청을 사용합니다.
- 개인 정보 및 민감한 사용자 데이터를 판매하지 않습니다.
  - '판매'란 개인 정보 및 민감한 사용자 데이터를 금전적인 대가를 받고 교환하거나 제3자 에게 전송하는 행위를 의미합니다.
    - 사용자가 개시한 개인 정보 및 민감한 사용자 데이터의 전송(예: 사용자가 앱의 기능을 사용해 제3자에게 파일을 전송하는 경우 또는 사용자가 조사 연구를 목적으로 하는 앱을 사용하기로 선택하는 경우)은 판매로 간주되지 않습니다.

명시적 공개 및 동의 요건

앱의 개인 정보 및 민감한 사용자 데이터 액세스, 수집, 사용 또는 공유가 해당 제품 또는 기능을 사용하는 사용자의 합리적인 기대 범위 내에 포함되지 않는 경우(예: 사용자가 앱을 사용하고 있지 않을 때 백그라운드에서 데이터가 수집되는 경우) 다음 요건을 충족해야 합니다.

명시적 공개: 데이터 액세스, 수집, 사용 및 공유 정보에 관한 인앱 공개를 제공해야 합니다. 인앱 공개는 다음 요건을 충족해야 합니다.

- 앱 설명 또는 웹사이트뿐만 아니라 앱 자체에도 있어야 합니다.
- 사용자가 일부러 메뉴나 설정으로 이동하지 않고도 일반적인 앱 사용 과정에서 볼 수 있어야 합니다.
- 액세스 또는 수집 중인 데이터를 설명해야 합니다.
- 데이터 사용 또는 공유 방법을 설명해야 합니다.
- 개인정보처리방침 또는 서비스 약관에만 포함되어서는 안 됩니다.
- 개인 정보 및 민감한 사용자 데이터 수집과 관련이 없는 다른 공개에 포함되어서는 안 됩니다.

동의 및 런타임 권한: 앱 내에서의 사용자 동의 요청 및 런타임 권한 요청은 이 정책의 요건을 충족하는 인앱 공개 직후에 이루어져야 합니다. 앱의 동의 요청은 다음 요건을 충족해야 합니다.

- 동의 대화상자를 명확하고 모호하지 않게 제시해야 합니다.
- 사용자가 동의 의사를 확실하게 표현하도록 요구해야 합니다(예: 탭하여 동의, 체크박스 선택).
- 공개 대화상자에서 나가는 행위(탭해서 나가기, 뒤로 버튼이나 홈 버튼 누르기 포함)를 동의로 해석해서는 안 됩니다.
- 자동 닫기 또는 만료 메시지를 사용자 동의 획득의 수단으로 사용해서는 안 됩니다.
- 사용자가 동의한 후에야 앱에서 개인 정보 및 민감한 사용자 데이터를 수집하거나 이러한 데이터에 액세스할 수 있습니다

EU GDPR에 따른 합법적 이해와 같이 다른 법적 근거를 이용해 동의 없이 개인 정보 및 민감한 사용자 데이터를 처리하는 앱은 해당 법적 요건을 모두 준수하고 이 정책에서 요구하는 바에 따라 인앱 공개 등을 통해 사용자에게 적절하게 공개해야 합니다.

정책 요건을 충족하기 위해 필요한 경우 다음과 같은 명시적 공개의 예시 형식을 참고할 것을 권장합니다.

- "[이 앱]은 [시나리오] 상황에서 ['기능']을 사용 설정하기 위해 [데이터 유형]을 수집/전송/동기화/저장합니다.
- *예: "Fitness Funds는 앱이 종료되었거나 사용 중이 아닌 상태에서도 피트니스 추적을 사용 설정하기 위해 위치 데이터를 수집하며 광고 지원에도 사용됩니다."*
- *예: "CallBuddy는 앱이 사용 중이 아닐 때에도 조직에 연락할 수 있도록 통화 기록 읽기 및 쓰기 데이터를 수집합니다."*

앱이 개인 정보 및 민감한 사용자 데이터를 기본적으로 수집하도록 만들어진 서드 파티 코드(예: SDK)를 통합하는 경우 Google Play에서 요청을 받은 후 2주 이내에(또는 Google Play가 요청에서 더 긴 기간을 제공한 경우 해당 기간 내에), 서드 파티 코드를 통한 데이터 액세스, 수집, 사용 또는 공유와 관련하여 앱이 본 정책의 명시적 공개 및 동의 요건을 준수한다는 사실을 보여주는 충분한 증거를 제공해야 합니다.

다음은 자주 발생하는 위반 사례입니다.

- 앱이 기기 위치를 수집하지만 명시적 공개를 통해 어떤 기능이 이 데이터를 사용하거나 앱의 백그라운드 사용을 표시하는지 설명하지 않습니다.
- 앱에 데이터의 사용 목적을 지정하는 명시적 공개 이전에 데이터 액세스를 요청하는 런타임 권한이 있습니다.
- 설치된 앱의 사용자 인벤토리에 액세스하며 이 데이터를 위의 개인정보처리방침, 데이터 취급과 명시적 공개 및 동의 요건이 적용되는 개인 정보 또는 민감한 정보로 취급하지 않습니다.
- 앱이 사용자의 전화번호부 또는 연락처 데이터에 액세스하며 이 데이터를 위의 개인정보처리방침, 데이터 취급과 명시적 공개 및 동의 요건이 적용되는 개인 정보 또는 민감한 정보로 취급하지 않습니다.
- 앱에서 사용자의 화면을 기록하고 이 데이터를 본 정책의 대상인 개인 정보 또는 민감한 정보로 취급하지 않습니다.
- 앱에서 기기 위치 를 수집하지만 위 요건에 따라 용도를 포괄적으로 공개하고 동의를 획득하지 않습니다.
- 앱이 추적, 조사, 마케팅 등의 목적으로 앱의 백그라운드에서 제한된 권한을 사용하지만 위 요건에 따라 용도를 포괄적으로 공개하거나 동의를 획득하지 않습니다.
- 앱이 SDK를 통해 개인 정보 및 민감한 사용자 데이터를 수집하지만 이러한 데이터를 이 사용자 데이터 정책, 액세스, 데이터 처리(허용되지 않는 판매 포함), 명시적 공개 및 동의 요건의 대상으로 취급하지 않습니다.

명시적 공개 및 동의 요건에 관한 자세한 내용은 이 도움말을 참고하세요.

개인 정보 및 민감한 정보 액세스 제한

아래 표에는 위 요건 외에 특정 활동과 관련된 요건이 설명되어 있습니다.

활동	요구사항
앱에서 금융 또는 결제 정보, 정부에서 발급한 신원 확인 번호를 처리하는 경우	앱은 금융 또는 결제 활동이나 모든 정부 발급 신원 확인 번호와 관련된 개인 정보 및 민감한 사용자 데이터를 절대로 공개하면 안 됩니다.
앱에서 비공개 연락처 목록 또는 연락처 정보를 처리하는 경우	사용자의 비공개 연락처를 무단으로 게시하거나 공개하는 것은 허용되지 않습니다.
앱에 바이러스 백신 또는 보안 기능(예: 바이러스 백신, 멀웨어 백신, 보안 관련 기능)이 포함된 경우	앱은 앱에서 수집 및 전송하는 사용자 데이터, 데이터 사용 방법 및 데이터가 공유되는 당사자 유형을 설명하는 개인정보처리방침과 모든 인앱 공개를 게시해야 합니다.
앱이 아동을 대상으로 하는 경우	아동 대상 서비스에 사용하도록 승인되지 않은 SDK를 앱에 포함해서는 안 됩니다. 정책 전문과 요건을 확인하려면 어린이와 가족을 위한 앱 설계 를 참고하세요.
앱이 영구적인 기기 식별자(예: IMEI, IMSI, SIM 일련번호 등)를 수집하거나 이에 연결하는 경우	영구적인 기기 식별자는 다음 용도를 제외하고는 다른 개인 정보 및 민감한 사용자 데이터 또는 재설정 가능한 기기 식별자와 연결할 수 없습니다. • SIM 아이덴티티와 연결된 전화 통신(예: 이동통신사 계정과 연결된 Wi-Fi 통화) 및 • 기기 소유자 모드를 사용하는 기업 기기 관리 앱 이러한 용도는 사용자 데이터 정책 에 명시된 대로 사용자에게 명확하게 공개되어야 합니다. 다른 고유 식별자에 관해 알아보려면 이 리소스를 참고 하세요. Android 광고 ID에 관한 추가 가이드라인은 광고 정책 에서 확인하세요.

데이터 보안 섹션

모든 개발자는 앱마다 사용자 데이터의 수집, 사용 및 공유에 관한 자세한 설명을 포함하여 데이터 보안 섹션을 명확하고 정확하게 작성해야 합니다. 개발자는 라벨을 정확히 작성하고 정보를 최신 상태로 유지할 책임이 있습니다. 해당하는 경우 데이터 보안 섹션은 앱의 개인정보처리방침에 공개된 내용과 일치해야 합니다.

데이터 보안 섹션을 완료하기 위한 추가 정보는 이 도움말 을 참고하세요.

개인정보처리방침

모든 앱은 Play Console의 지정된 필드에 개인정보처리방침 링크를, 앱 자체에는 개인정보처리방침 링크 또는 텍스트를 게시해야 합니다. 개인정보처리방침에서는 모든 인앱 공개와 더불어 앱의 사용자 데이터 액세스, 수집, 사용, 공유 방식을 포괄적으로 공개해야 하며, 이는 데이터 보안 섹션에 공개된 데이터로 국한되지 않습니다. 여기에는 다음 정보가 포함되어야 합니다.

- 개발자 정보 및 개인 정보 보호 담당자 또는 문의사항 제출 메커니즘
- 앱에서 액세스, 수집, 사용, 공유하는 개인 정보 및 민감한 사용자 데이터 유형과 개인 정보 또는 민감한 사용자 데이터를 공유하는 모든 주체 공개
- 개인 정보 및 민감한 사용자 데이터를 안전하게 처리하는 절차
- 개발자의 데이터 보관 및 삭제 정책
- 개인정보처리방침이라는 명확한 라벨 지정(예: 제목에 '개인정보처리방침'을 명시)

앱의 Google Play 스토어 등록정보에 명시된 법인(예: 개발자, 회사)이 개인정보처리방침에 언급되거나 앱의 이름이 개인정보처리방침에 명시되어야 합니다. 개인 정보 및 민감한 사용자 데이터에 액세스하지 않는 앱도 개인정보처리방침을 제출해야 합니다.

개인정보처리방침이 PDF가 아닌 공개적으로 액세스 가능하고 지오펜싱되지 않은 URL을 통해 실제로 접속할 수 있으며 수정 불가능한지 확인하시기 바랍니다.

계정 삭제 요건

사용자가 앱 내에서 계정을 만들 수 있는 경우 계정 삭제를 요청할 수도 있어야 합니다. 사용자는 앱 내에서, 그리고 외부(예: 웹사이트 방문 등)에서 앱 계정 삭제를 시작하는 옵션을 바로 찾을 수 있어야 합니다. Play Console 내의 지정된 URL 양식 필드에 이 웹 리소스 링크를 입력해야 합니다.

사용자의 요청에 따라 앱 계정을 삭제할 때는 앱 계정과 관련된 사용자 데이터도 삭제해야 합니다. 일시적 계정 비활성화, 사용 중지 또는 앱 계정 '정지'는 계정 삭제로 인정되지 않습니다. 보안, 사기 방지 또는 규정 준수 등 정당한 사유로 특정 데이터를 보관해야 하는 경우 사용자에게 데이터 보관 관행을 명확하게 알려야 합니다(예: 개인정보처리방침 등에서).

계정 삭제 정책 요구사항에 관해 자세히 알아보려면 이 고객센터 도움말을 참고하세요. 데이터 보안 양식 업데이트에 관한 추가 정보는 이 도움말을 참고하세요.

앱 설정 ID 사용 사례

Android는 분석, 사기 방지와 같은 필수 사용 사례를 지원하기 위해 새로운 ID를 도입할 예정입니다. 이러한 ID 사용에 관한 조건은 아래와 같습니다.

- **용도**: 앱 설정 ID는 광고 개인 최적화 및 광고 측정에 사용되어서는 안 됩니다.
- **개인 식별 정보 또는 기타 식별자와 연결:** 앱 세트 ID는 광고 목적으로 AAID와 같은 Android 식별자나 다른 개인 정보 및 민감한 정보와 연결되어서는 안 됩니다.
- **투명성 및 동의:** 앱 설정 ID의 수집과 사용 및 이러한 조건을 준수한다는 확약은 개인정보처리방침을 비롯해 법적으로 적합한 개인 정보 보호 고지를 통해 사용자에게 공개되어야 합니다. 필요한 경우 사용자로부터 유효한 법적 동의를 얻어야 합니다. Google의 개인 정보 보호 표준을 자세히 알아보려면 사용자 데이터 정책 을 검토하세요.

EU-미국, 영국 및 스위스 데이터 개인 정보 보호 프레임워크

귀하가 Google을 통해 제공되며 개인을 직접적 또는 간접적으로 식별하는 개인 정보에 액세스하거나, 이를 사용하거나, 처리하며 이 정보의 출처가 유럽 경제 지역, 영국, 또는 스위스('유럽연합 개인 정보')인 경우에는 다음 사항을 준수해야 합니다.

- 모든 개인 정보 보호, 데이터 보안, 데이터 보호 관련 법, 지침, 규정, 규칙을 준수해야 합니다.
- EU 개인정보와 관련된 개인이 동의한 내용과 일치하는 목적으로만 EU 개인정보에 액세스하거나 이를 사용 또는 처리해야 합니다.
- 개인 정보의 분실, 오용, 무단 또는 불법 액세스, 공개, 변경, 파기에 대비하여 EU 개인 정보를 보호할 적절한 조직과 기술 수단을 구현해야 합니다.
- 데이터 개인 정보 보호 프레임워크 원칙 에서 요구하는 수준의 보안 또는 Google 컨트롤러 간 데이터 보호 약관의 설명에 따라 관련 전송 메커니즘을 제공해야 합니다.

귀하는 이러한 조건이 충족되는지 정기적으로 모니터링해야 합니다. 이러한 조건을 충족할 수 없는 경우(또는 충족하지 못할 상당한 위험이 있는 경우) 언제든지 data-protection-office@google.com 으로 이메일을 보내 Google에 바로 알려야 하며, EU 개인 정보의 처리를 즉시 중지하거나 합당한 보호 수준을 복구하기 위해 합리적이고 적절한 조치를 취해야 합니다.

민감한 정보에 액세스하는 권한 및 API

민감한 정보 액세스 권한 및 API에 관한 요청은 사용자가 이해할 수 있어야 합니다. Google Play 등록정보에서 홍보된 앱의 현재 기능 또는 서비스를 구현하는 데 필요한 민감한 정보 액세스 권한 및 API만 요청할 수 있습니다. 공개, 구현 또는 허용되지 않은 기능이나 목적을 위해 사용자 또는 기기 데이터에 액세스하는 민감한 정보 액세스 권한 또는 API를 사용해서는 안 됩니다. 민감한 정보에 액세스하는 권한 또는 API를 통해 액세스한 개인 정보 또는 민감한 정보는 절대로 판매하거나 판매를 촉진할 목적으로 공유할 수 없습니다.

사용자가 앱에서 권한을 요청하는 이유를 이해할 수 있도록 권한을 단계별로 요청하여 관련 맥락 안에서 데이터에 액세스할 민감한 정보 액세스 권한 및 API를 요청합니다. 데이터를 사용자가 동의한 목적으로만 사용합니다. 추후 데이터를 다른 용도로 사용하려면 이러한 추가 사용에 대해 사용자의 명확한 동의를 반드시 받아야 합니다.

제한된 권한

위에 명시된 내용에 더해 제한된 권한이라는 개념이 있습니다. 이러한 권한은 위험 , 특수 , 서명 또는 아래 설명된 바와 같이 지정됩니다. 이러한 권한에는 다음과 같은 추가 요건과 제한사항이 적용됩니다.

- 제한된 권한을 통해 액세스되는 사용자 또는 기기 데이터는 개인 정보 및 민감한 사용자 데이터로 간주됩니다. 사용자 데이터 정책 의 요건이 적용됩니다.
- 제한된 권한 요청을 거부할 경우 사용자의 결정을 존중해야 하며, 사용자가 중요하지 않은 권한에 동의하도록 유도하거나 강요해서는 안 됩니다. 민감한 권한에 대한 액세스를 허용하지 않은 사용자도 앱을 이용할 수 있도록 합당한 노력을 기울여야 합니다. 예를 들어 사용자가 통화 기록 액세스를 제한한 경우 전화번호를 수동으로 입력할 수 있도록 합니다.
- Google Play 멀웨어 정책 을 위반하여 권한을 사용하는 행위(승격된 권한 남용 포함)는 명시적으로 금지됩니다.

특정 제한된 권한은 아래에 설명된 추가 요건의 적용을 받을 수 있습니다. 이러한 제한사항의 목적은 사용자의 개인 정보를 보호하는 데 있습니다. 아주 드문 경우이지만, 앱이 매우 강력하거나 중요한 기능을 제공하고 그 기능을 제공할 다른 방법이 없으면 아래의 요건에 제한적으로 예외를 허용할 수 있습니다. Google은 개인 정보 보호 또는 보안 측면에서 사용자가 받을 수 있는 영향을 고려하여 예외 적용 여부를 평가합니다.

SMS 및 통화 기록 권한

SMS 및 통화 기록 권한은 개인 정보와 민감한 정보 정책에 따라 개인 정보 및 민감한 사용자 데이터로 간주되며 다음 제한사항이 적용됩니다.

제한된 권한	요구사항
통화 기록 권한 그룹(예: READ_CALL_LOG, WRITE_CALL_LOG, PROCESS_OUTGOING_CALLS)	앱이 현재 기기에서 기본 전화 또는 어시스턴트 핸들러로 등록되어 있어야 합니다.
SMS 권한 그룹(예: READ_SMS, SEND_SMS, WRITE_SMS, RECEIVE_SMS, RECEIVE_WAP_PUSH, RECEIVE_MMS)	앱이 현재 기기에서 기본 SMS 또는 어시스턴트 핸들러로 등록되어 있어야 합니다.

기본 SMS, 전화 또는 어시스턴트 핸들러 기능이 없는 앱은 매니페스트에서 위 권한의 사용을 선언할 수 없습니다. 여기에는 매니페스트의 자리표시자 텍스트도 포함됩니다. 또한, 앱이 사용자에게 위의 권한을 허용해 달라는 메시지를 표시하기 전에 현재 기본 SMS, 전화 또는 어시스턴트 핸들러로 등록되어 있어야 하며 더 이상 기본 핸들러가 아닌 경우에는 권한 사용을 즉시 중지해야 합니다. 허용된 사용 및 예외 사례는 이 고객센터 페이지 에 있습니다.

앱은 승인된 핵심 앱 기능을 제공하기 위한 목적으로만 권한(및 권한에서 파생된 모든 데이터)을 사용할 수 있습니다. 핵심 기능이란 앱의 주요 목적으로 정의됩니다. 여기에는 핵심 기능의 조합이 포함되며, 핵심 기능은 앱에 관한 설명에서 가장 두드러지게 소개 및 홍보된 기능을 말합니다. 핵심 기능이 제공되지 않으면 앱은 '기능이 부족한' 앱이 되거나 사용할 수 없게 됩니다. 이 데이터의 전송, 공유 또는 라이선스가 부여된 사용은 앱 내의 핵심 기능이나 서비스를 제공하기 위한 용도로만 이루어져야 하며, 다른 목적(예: 다른 앱이나 서비스 개선, 광고 또는 마케팅 목적)으로 사용을 확장할 수 없습니다. 통화 기록 또는 SMS 관련 권한에 따른 데이터를 파생시키기 위해 다른 방법(다른 권한, API 또는 제3자 소스)을 사용할 수 없습니다.

위치 정보 액세스 권한

기기 위치 는 개인 정보 및 민감한 정보 정책, 백그라운드 위치 액세스 정책에 따라 개인 정보 및 민감한 사용자 데이터로 간주되며 다음 요구사항이 적용됩니다.

- 앱의 현재 기능이나 서비스를 제공하는 데 더 이상 필요하지 않으면 앱에서 위치 정보 액세스 권한(예: ACCESS_FINE_LOCATION, ACCESS_COARSE_LOCATION, ACCESS_BACKGROUND_LOCATION)으로 보호되는 데이터에 액세스해서는 안 됩니다.
- 광고 또는 분석 목적으로만 사용자에게 위치 정보 액세스 권한을 요청해서는 안 됩니다. 앱에서 광고 게재를 위해 허용되는 위치 데이터 사용 사례를 확장할 경우 Google의 광고 정책 을 준수해야 합니다.
- 앱은 위치가 필요한 현재 기능 또는 서비스를 제공하기 위해 필요한 최소 범위(즉, 미세한 수준 대신 대략적 수준, 백그라운드 대신 포그라운드)를 요청해야 하며, 사용자가 기능 또는 서비스에 요청된 위치 수준이 필요하다고 합리적으로 예상할 수 있어야 합니다. 예를 들어 Google에서는 강력한 근거 없이 백그라운드 위치를 요청하거나 이 위치에 액세스하는 앱을 거부할 수 있습니다.
- 백그라운드 위치 액세스는 사용자에게 유용하며 앱의 핵심 기능과 관련이 있는 기능을 제공하는 용도로만 사용할 수 있습니다.

앱에서는 다음에 해당하는 경우 포그라운드 서비스(앱에 포그라운드 액세스 권한만 있는 경우, 예: '사용 중에만') 권한을 사용하여 위치에 액세스할 수 있습니다.

- 위치의 사용이 사용자가 시작한 인앱 작업의 연장으로 시작된 경우
- 애플리케이션에서 사용자 시작 작업이 의도된 목적대로 완료된 직후 위치의 사용이 종료되는 경우

아동을 대상으로 만들어진 앱은 가족을 위한 앱 정책을 준수해야 합니다.

정책 요구사항에 관한 자세한 내용은 이 도움말 을 참고하세요.

모든 파일 액세스 권한

사용자 기기의 파일과 디렉터리 속성은 개인 정보 및 민감한 정보 정책에 따라 개인 데이터 및 민감한 사용자 데이터로 간주되며 다음 요건이 적용됩니다.

- 앱은 작동하는 데 필수적인 기기 스토리지에만 액세스 권한을 요청해야 하며, 사용자에게 표시되는 중요한 기능과 관련이 없는 목적으로 제3자를 대신하여 기기 스토리지에 액세스 권한을 요청할 수 없습니다.
- 공유 저장공간의 액세스 권한을 관리하려면 R 이상을 실행하는 Android 기기에 MANAGE_EXTERNAL_STORAGE 권한이 필요합니다. R을 타겟팅하고 공유 스토리지에 관한 폭넓은 액세스 권한('모든 파일 액세스')을 요청하는 모든 앱은 게시 전에 적절한 액세스 검토를 반드시 통과해야 합니다. 이 권한을 사용하도록 허용된 앱은 '특수 앱 액세스' 설정에 따라 앱에 '모든 파일 액세스'를 사용 설정하도록 사용자에게 분명하게 메시지를 표시해야 합니다. R 요건에 관한 자세한 내용은 이 도움말 을 참고하세요.

패키지(앱) 가시성 권한

기기에서 쿼리되는 설치된 앱의 인벤토리는 개인 정보 및 민감한 정보 정책이 적용되는 개인 데이터 및 민감한 사용자 데이터로 간주되며, 다음 요구사항이 적용됩니다.

기기 내 다른 앱의 실행, 검색 또는 다른 앱과의 상호 운용이 핵심 목적인 앱은 아래에 간략히 설명된 것처럼 적합한 범위 내에서 기기에 설치된 다른 앱을 확인할 수 있습니다.

- **광범위한 가시성:** 광범위한 가시성은 앱이 기기에 설치된 앱('패키지')을 폭넓게(또는 '광범위하게') 확인할 수 있는 기능입니다.
  - API 수준 30 이상 을 타겟팅하는 앱의 경우 QUERY_ALL_PACKAGES 권한을 통해 부여된 광범위한 가시성은 앱이 작동하기 위해 기기 내 모든 앱을 인지하거나 이와 상호작용해야 하는 특정 사용 사례로 제한됩니다.
    - 앱이 범위가 더 정확히 타겟팅된 패키지 가시성 선언 만으로도 작동 가능한 경우 QUERY_ALL_PACKAGES를 사용할 수 없습니다. 예를 들어, 광범위한 가시성을 요청하는 대신 특정 패키지를 쿼리하고 이와 상호작용하는 경우가 여기에 해당합니다.
  - 대체 메서드를 사용하여 QUERY_ALL_PACKAGES 권한과 관련된 광범위한 가시성을 대략적으로 얻을 수 있는데, 이 또한 사용자를 대상으로 한 핵심 앱 기능과 이 메서드를 통해 발견된 모든 앱과의 상호 운용으로 제한됩니다.
  - QUERY_ALL_PACKAGES 권한이 허용되는 사용 사례를 알아보려면 이 고객센터 도움말 을 참고하세요.
- **제한된 앱 가시성**: 제한된 가시성은 앱이 더 정확하게 타겟팅된('광범위'하지 않음) 메서드를 사용하여 특정 앱을 쿼리함으로써 데이터 액세스를 최소화합니다. 예를 들어, 앱의 매니페스트 선언에 맞는 특정 앱을 쿼리하는 경우가 여기에 해당합니다. 앱이 정책을 준수하는 방식으로 상호 운용되거나 이러한 앱을 관리하는 경우 이 메서드를 사용하여 앱을 쿼리할 수 있습니다.
- 기기에 설치된 앱의 인벤토리에 대한 가시성은 사용자가 앱 내에서 액세스하는 핵심 기능이나 앱의 핵심 목적과 직접적인 관련이 있어야 합니다.

Play를 통해 배포된 앱에서 쿼리되는 앱 인벤토리 데이터는 분석 또는 광고 수익 창출 목적으로 판매되거나 공유되어서는 안 됩니다

Accessibility API

Accessibility API는 다음과 같은 용도로 사용할 수 없습니다.

- 사용자의 허락 없이 사용자 설정을 변경하거나 사용자가 앱 또는 서비스를 사용 중지하거나 제거할 수 있는 기능 차단(자녀 보호 기능 앱을 통해 부모 또는 보호자로부터 승인을 받았거나 기업 관리 소프트웨어를 통해 권한이 있는 관리자로부터 승인을 받은 경우 제외)
- Android에서 기본 제공하는 개인 정보 보호 설정 및 알림 우회
- 사기성이 있거나 그 밖의 Google Play 개발자 정책을 위반하는 방식으로 사용자 인터페이스 변경 또는 활용

Accessibility API는 원격 통화 녹음을 위해 만들어지지 않았으며 이 목적으로 해당 API를 요청할 수 없습니다.

Accessibility API 사용은 Google Play 등록정보에 명시해야 합니다.

IsAccessibilityTool 가이드라인

장애인 직접 지원이 핵심 기능인 앱은 **IsAccessibilityTool**을 사용하여 공개적이며 적절한 방식을 사용해 직접 접근성 앱임을 지정할 수 있습니다.

IsAccessibilityTool 사용 자격이 없는 앱은 이 라벨을 사용할 수 없으며, 사용자가 접근성과 관련된 기능을 명확하게 알 수 없으므로 사용자 데이터 정책 에 설명된 명시적 공개 및 동의 요건을 충족해야 합니다. 자세한 정보는 AccessibilityService API 고객센터 도움말을 참고하세요.

Accessibility API를 사용하지 않고도 필요한 기능을 제공할 수 있다면 더 범위를 좁혀 제한된 API 및 권한 을 사용해야 합니다.

패키지 설치 요청 권한

REQUEST_INSTALL_PACKAGES 권한이 있으면 애플리케이션에서 앱 패키지 설치를 요청할 수 있습니다. 이 권한을 사용하려면 앱의 핵심 기능에 다음이 모두 포함되어야 합니다.

- 앱 패키지 전송 또는 수신
- 사용자가 시작하는 앱 패키지 설치 지원

허용되는 기능은 다음과 같습니다.

- 웹 탐색 또는 검색
- 첨부파일을 지원하는 커뮤니케이션 서비스
- 파일 공유, 전송 또는 관리
- 엔터프라이즈 기기 관리
- 백업 및 복원
- 기기 이전/전화 연결
- 휴대전화를 웨어러블 또는 IoT 기기에 동기화하는 호환 앱(예: 스마트시계 또는 스마트 TV)

핵심 기능은 앱의 기본 목적으로 정의됩니다. 핵심 기능은 물론, 이 핵심 기능을 구성하는 모든 핵심 기능이 앱 설명에서 명확하게 소개 및 홍보되어야 합니다.

기기 관리 목적이 아닌 한 자체 업데이트, 수정 또는 애셋 파일에서 다른 APK와의 번들 구성을 위해 REQUEST_INSTALL_PACKAGES 권한을 사용할 수 없습니다. 모든 업데이트 또는 패키지 설치는 Google Play의 기기 및 네트워크 악용 정책을 준수해야 하며 사용자가 시작하고 구동해야 합니다.

Health Connect by Android 권한

헬스 커넥트 는 건강/피트니스 앱이 통합 생태계 내에서 동일한 온디바이스 데이터를 저장하고 공유할 수 있도록 허용하는 Android 플랫폼입니다. 이를 통해 사용자는 건강 기록을 비롯해 건강/피트니스 데이터의 읽기 및 쓰기가 가능한 앱을 한곳에서 제어할 수 있습니다. 건강 기록에는 의료 기록, 진단, 처치, 약물, 검사 결과나 의료인 또는 기관으로부터 또는 지원되는 서드 파티 건강 플랫폼을 통해 획득한 기타 임상 데이터가 포함될 수 있습니다.

헬스 커넥트는 걸음 수, 체온, 건강 기록 데이터 등 다양한 데이터 유형 의 읽기 및 쓰기를 지원합니다.

헬스 커넥트 권한을 통해 액세스되는 데이터는 사용자 데이터 정책이 적용되는 개인 정보 및 민감한 사용자 데이터로 간주됩니다. 앱이 건강 앱에 해당하거나, 건강 관련 기능을 제공하면서 헬스 커넥트 데이터를 비롯한 건강 데이터에 액세스하는 경우 건강 앱 정책도 준수해야 합니다.

헬스 커넥트를 시작하는 방법에 관해서는 이 Android 개발자 가이드 를 참고하세요. 헬스 커넥트 데이터 유형에 대한 액세스 및 기타 FAQ를 요청하려면 헬스 커넥트 정책 요구사항 FAQ를 참고하세요.

Google Play를 통해 배포된 앱은 헬스 커넥트 데이터 읽기 및/또는 쓰기가 가능하려면 다음과 같은 정책 요구사항을 충족해야 합니다.

적절한 Health Connect 액세스 권한 및 사용

헬스 커넥트는 본 정책에 명시되어 있는 승인된 사용 사례에 한해 해당하는 정책과 이용약관에 따라서만 사용할 수 있습니다. 즉, 애플리케이션 또는 서비스가 승인된 사용 사례 중 하나를 충족하는 경우에만 권한 액세스를 요청할 수 있습니다.

승인된 사용 사례로는 피트니스 및 웰빙, 보상, 피트니스 코칭, 기업 웰니스, 의료, 건강 연구, 게임이 포함됩니다. 이러한 사용 사례에 대한 액세스가 부여된 애플리케이션은 공개되지 않거나 허용되지 않은 목적으로 용도를 확대할 수 없습니다.

사용자의 건강 및 피트니스에 도움이 되도록 설계된 기능을 하나 이상 갖춘 애플리케이션 또는 서비스만 헬스 커넥트 권한에 대한 액세스를 요청할 수 있습니다. 예를 들면 다음과 같습니다.

- 사용자가 신체 활동, 수면, 정신 건강, 영양, 건강 측정 정보, 신체 상태 설명, 건강 기록 및/또는 기타 건강 또는 피트니스 관련 설명 및 측정 정보를 **바로 기록, 보고, 모니터링 및/또는 분석**할 수 있는 애플리케이션 또는 서비스
- 사용자가 **신체 활동, 수면, 정신 건강, 영양, 건강 측정 정보, 신체 상태 설명, 건강 기록** 및/또는 기타 건강 또는 피트니스 관련 설명 및 측정 정보를 기기에 **저장**하고 이러한 사용 사례를 충족하는 기기 내 기타 앱과 데이터를 공유할 수 있는 애플리케이션 또는 서비스
- 사용자가 만성 질환, 의료적 처치 또는 치료 지원을 관리할 수 있는 애플리케이션 또는 서비스

헬스 커넥트 액세스 권한은 본 정책 또는 기타 관련 헬스 커넥트 이용약관 또는 정책을 위반하는 방식으로 사용할 수 없으며, 여기에는 다음 목적이 포함됩니다.

- 헬스 커넥트의 사용 또는 오류로 인해 사망, 부상, 개인에 대한 피해 또는 환경이나 재산 피해가 발생할 것이 합리적으로 예상할 수 있는 경우(예: 핵시설, 항공 관제소, 인명 구조 시스템 또는 무기의 제작 또는 운영) 애플리케이션, 환경 또는 활동을 개발하는 데 헬스 커넥트를 사용하거나 그러한 대상에 통합하지 마십시오.
- 헬스 커넥트를 통해 얻은 데이터에 헤드리스 앱을 사용하여 액세스하지 마십시오. 앱은 앱 트레이, 기기 앱 설정, 알림 아이콘 등에 명확하게 식별 가능한 아이콘을 표시해야 합니다.
- 비호환 기기 또는 플랫폼 간에 데이터를 동기화하는 앱과 함께 헬스 커넥트를 사용하지 마십시오.
- 어린이만을 타겟팅하는 애플리케이션, 서비스 또는 기능에 연결하는 데 헬스 커넥트를 사용하면 안 됩니다.
- 무단 또는 불법적인 액세스, 사용, 파괴, 손실, 변형 또는 공개에 합당하고 적절한 조치를 취하여 헬스 커넥트를 사용하는 모든 애플리케이션 또는 시스템을 보호합니다.

또한 귀하에게는 헬스 커넥트 및 헬스 커넥트에서 얻은 데이터의 의도된 사용에 따라 적용될 수 있는 모든 규정 또는 현지 법규를 준수할 책임이 있습니다. 예를 들어 건강 보험 이동성 및 책임법(HIPAA)에 따른 적용 대상 또는 비즈니스 제휴사인 경우 헬스 커넥트의 정보에 액세스하고 이를 활용하려면 관련 요구사항을 준수해야 합니다. EU 사용자를 대상으로 개인 정보 보호법(GDPR)이 적용되는 개발자인 경우 마찬가지로 GDPR에 따른 의무를 준수해야 합니다. 이러한 법률 및 규정에 따라 귀하의 처리 활동에 관여하는 관련 기관과 데이터를 공유하기 전에 추가적인 계약(예: 비즈니스 제휴 계약 또는 데이터 처리 계약)을 체결해야 할 수 있습니다. 활동에 이러한 계약이 필요한지 여부를 판단하는 것 또한 앱 개발자의 책임입니다. 개발자는 Google에서 요청 시 이러한 계약 또는 규정 준수에 관한 증빙을 Google에 제공해야 합니다.

특정 Google 제품 또는 서비스에 대해 Google이 제공하는 라벨 또는 정보에 명시적으로 기록된 경우를 제외하고 Google은 특히 연구, 보건 또는 의료 용도를 비롯해 어떠한 용도 또는 목적으로도 헬스 커넥트에 포함된 데이터의 사용을 보증하거나 이러한 데이터의 정확성을 보장하지 않습니다. Google은 헬스 커넥트를 통해 획득한 데이터의 사용과 관련된 모든 책임을 부인합니다.

용도 제한

헬스 커넥트 사용 시에는 다음과 같은 특정한 제한에 따라 데이터에 액세스하고 이를 사용해야 합니다.

- 데이터 사용은 애플리케이션의 사용자 인터페이스에 표시되는 적절한 사용 사례 또는 기능을 제공하고 개선하는 목적으로 제한되어야 합니다.

- 사용자 데이터는 명시적인 사용자 동의가 있는 경우에 보안 목적(예: 악용 조사), 관련 법률 또는 규정 준수, 인수/합병과 같은 목적으로만 제3자에게 전송할 수 있습니다.
- 명시적인 사용자 동의가 없는 경우 사용자 데이터에 대한 사람의 액세스는 보안 목적, 법률 준수 또는 현지 법규에 따른 내부 운영을 위한 합산 목적으로 제한됩니다.
- **기타 모든 헬스 커넥트 데이터의 전송, 사용 또는 판매는 금지되며, 여기에는 다음이 포함됩니다.**
  - 광고 플랫폼, 데이터 중개업체 또는 정보 리셀러 같은 제3자에게 사용자 데이터를 전송 또는 판매하는 행위
  - 개인 맞춤 광고 또는 관심 기반 광고 등 광고를 게재하기 위해 사용자 데이터를 전송, 판매 또는 사용하는 행위
  - 신용도를 판단하거나 대출을 목적으로 사용자 데이터를 전송, 판매 또는 사용하는 행위
  - 의료 기기의 자격을 충족할 수 있는 제품 또는 서비스를 통해 사용자 데이터를 전송, 판매 또는 사용하는 행위(의료 기기 앱에서 헬스 커넥트 데이터를 사용하고자 하는 용도로 관련성 높은 규제 기관(예: 미국 식품의약청)으로부터 필요한 모든 승인 또는 허가를 받는 등 모든 관련 규정을 준수하며 사용자가 그러한 사용에 관해 명시적으로 동의한 경우 제외)
  - 사용자가 시작하거나 HIPAA 규정을 준수하는 경우를 제외하고 보호 건강 정보(HIPAA의 정의에 따름)와 관련된 목적 또는 방식으로 사용자 데이터를 전송, 판매 또는 사용하는 행위

최소 범위

제품의 기능 또는 서비스 구현 권한에 대한 액세스만 요청해야 합니다. 이러한 액세스 권한 요청은 구체적이고 필요한 데이터로만 국한되어야 합니다.

투명하고 정확한 공지 및 제어

헬스 커넥트는 건강 및 피트니스 데이터를 처리하며, 여기에는 개인 정보 및 민감한 정보가 포함됩니다. 개발자는 종합적인 개인정보처리방침을 통해 데이터 관행에 관한 명확하고 쉽게 접근 가능한 공개 정보를 제공해야 합니다. 이러한 공개 정보에는 다음이 포함되어야 합니다.

- 사용자 데이터에 대한 액세스를 요청하는 애플리케이션 또는 서비스의 정체성에 관한 정확한 표현.
- 액세스, 요청 및/또는 수집 대상 데이터의 유형을 명확하고 정확하게 설명하는 정보. 데이터는 앱에서 제공하는 사용자 대상 기능 또는 추천과 관련이 있어야 합니다.
- 데이터의 사용 및/또는 공유 방식에 관한 설명. 한 가지 이유로 요청한 데이터를 부차적 목적으로도 사용할 경우, 모든 사용 사례를 사용자에게 공개해야 합니다.
- 사용자가 데이터를 관리하고 앱에서 삭제할 방법 및 계정 비활성화 및/또는 삭제 시 데이터에 발생하는 일을 설명하는 사용자 도움말 문서.
- 전송에 최신 암호화 기술(예: HTTPS 연결)을 사용하는 등 모든 개인 정보 및 민감한 사용자 데이터의 안전한 처리 작업과 관련된 정보.

앱을 헬스 커넥트에 연결하기 위한 요건을 자세히 알아보려면 이 고객센터 도움말을 참고하시기 바랍니다.

VPN 서비스

VpnService 는 애플리케이션에서 자체 VPN 솔루션을 확장하고 구축하기 위한 기본 클래스입니다. VpnService를 사용하고 VPN을 핵심 기능으로 하는 앱만이 원격 서버에 대한 기기 수준의 보안 터널을 생성할 수 있습니다. 다음과 같은 핵심 기능을 위해 원격 서버가 필요한 앱은 예외입니다.

- 자녀 보호 기능 및 기업 관리 앱
- 앱 사용 추적
- 기기 보안 앱(예: 바이러스 백신, 휴대기기 관리, 방화벽)
- 네트워크 관련 도구(예: 원격 액세스)
- 웹 브라우징 앱
- 전화 통신 또는 연결 서비스를 제공하기 위해 VPN 기능을 사용해야 하는 이동통신사 앱

VpnService는 다음과 같은 용도로 사용할 수 없습니다.

- 명시적 공개 및 동의 없이 개인 정보 및 민감한 사용자 데이터 수집

- 수익 창출을 위해 기기에서 다른 앱의 사용자 트래픽을 리디렉션하거나 조작(예:사용자의 거주국이 아닌 국가를 통해 광고 트래픽을 리디렉션하는 경우)

VpnService를 사용하는 앱은 다음 사항을 모두 준수해야 합니다.

- Google Play 등록정보에 VpnService 사용 명시
- 기기에서 VPN 터널 엔드포인트까지 데이터 암호화
- 광고 사기 , 권한 , 멀웨어 정책 등 모든 개발자 프로그램 정책 준수

정확한 알람 권한

Android 13(API 타겟 수준 33)부터 앱에서 정확한 알람 기능 에 대한 액세스 권한을 부여하는 새로운 권한인 USE_EXACT_ALARM이 도입됩니다.

USE_EXACT_ALARM은 제한된 권한이며, 앱은 핵심 기능이 정확한 알람의 필요에 부합하는 경우에만 이 권한을 선언해야 합니다. 이 제한된 권한을 요청하는 앱은 검토를 거치며, 허용되는 사용 사례 기준을 충족하지 못한 앱은 Google Play에 게시할 수 없습니다.

정확한 알람 권한 사용을 위해 허용되는 사용 사례

앱의 사용자 대상 핵심 기능에 다음과 같이 시간을 정확하게 지키는 작업이 필요한 경우에만 앱에서 USE_EXACT_ALARM 기능을 사용해야 합니다.

- 앱이 알람 또는 타이머 앱입니다.
- 앱이 이벤트 알림을 표시하는 캘린더 앱입니다.

위에서 다루지 않았으나 정확한 알람 기능이 필요한 사용 사례가 있는 경우 대안으로 SCHEDULE_EXACT_ALARM의 사용을 고려해 보아야 합니다.

정확한 알람 기능에 관한 자세한 내용은 이 개발자 가이드 를 참고하세요.

전체 화면 인텐트 권한

Android 14(대상 API 수준 34) 이상을 타겟팅하는 앱의 경우 USE_FULL_SCREEN_INTENT 는 특수 앱 액세스 권한 입니다. 높은 우선순위의 알림이 필요한 아래 카테고리 중 하나에 앱의 핵심 기능이 해당하는 경우에만 USE_FULL_SCREEN_INTENT 사용 권한이 앱에 자동으로 부여됩니다.

- 알람 설정
- 전화 또는 영상 통화 수신

이 권한을 요청하는 앱은 검토를 거치며 위 기준을 충족하지 못한 앱에는 권한이 자동으로 부여되지 않습니다. 이 경우 앱에서 USE_FULL_SCREEN_INTENT를 사용하려면 사용자에게 권한을 요청해야 합니다.

USE_FULL_SCREEN_INTENT 권한 사용 시 원치 않는 모바일 소프트웨어, 기기 및 네트워크 악용, 광고 정책을 포함한 모든 Google Play 개발자 정책을 준수해야 함에 유의해 주시기 바랍니다. 전체 화면 인텐트 알림이 사용자 기기를 방해하거나, 중단 또는 손상시키거나 기기에 무단으로 액세스해서는 안 됩니다. 또한 앱은 다른 앱 또는 기기의 사용성을 방해하지 않아야 합니다.

고객센터에서 USE_FULL_SCREEN_INTENT 권한에 관해 자세히 알아보세요.

기기 및 네트워크 악용

사용자의 기기, 기타 기기 또는 컴퓨터, 서버, 네트워크, 애플리케이션 프로그래밍 인터페이스(API), 서비스(기기에 설치된 기타 앱, Google 서비스, 승인된 이동통신사 네트워크를 포함하나 이에 국한되지 않음)를 방해하거나, 작동에 지장을 주거나, 손상하거나, 무단으로 액세스하는 앱은 허용되지 않습니다.

Google Play의 앱은 Google Play의 핵심 앱 품질 가이드라인 에 명시된 기본 Android 시스템 최적화 요구사항을 준수해야 합니다.

Google Play를 통해 배포된 앱은 Google Play의 업데이트 메커니즘 이외의 방법을 사용하여 자체적으로 수정, 대체 또는 업데이트할 수 없습니다. 또한 Google Play가 아닌 다른 출처에서 dex, JAR, .so 파일 등의 실행 코드를 다운로드할 수 없습니다. 이러한 제한사항은, 가상 머신 또는 인터프리터가 Android API에 간접적으로 액세스할 수

있게 해 주는 경우(예: WebView 또는 브라우저에서 실행되는 자바스크립트) 그러한 가상 머신 또는 인터프리터에서 실행되는 코드에는 적용되지 않습니다.

런타임에 로드된(예: 앱과 패키징되지 않은) 인터프리트 언어(자바스크립트, Python, Lua 등)가 포함된 앱 또는 제3자 코드(예: SDK)에서 잠재적인 Google Play 정책 위반을 허용해서는 안 됩니다.

보안 취약점을 야기하거나 악용하는 코드는 허용되지 않습니다. 개발자에게 신고된 최근 보안 문제에 관해 알아보려면 앱 보안 개선 프로그램 을 확인하세요.

다음은 자주 발생하는 위반 사례입니다.

일반적인 기기 및 네트워크 악용 위반의 예는 다음과 같습니다.

- 광고를 표시하는 다른 앱을 차단하거나 방해하는 앱
- 다른 앱의 게임플레이에 영향을 미치는 게임 속임수 앱
- 서비스, 소프트웨어 또는 하드웨어를 해킹하거나 보안 기능을 우회하는 방법을 조장하거나 안내하는 앱
- 서비스 약관을 위반하는 방식으로 서비스 또는 API에 액세스하거나 이를 사용하는 앱
- 허용 목록에 포함 할 수 없고 시스템 전원 관리 를 우회하려고 시도하는 앱
- 서드 파티에게 프록시 서비스를 제공하는 앱은 사용자를 대상으로 이러한 기능을 제공하는 것이 앱의 주된 목적인 경우에만 서비스를 제공할 수 있습니다.
- Google Play 이외의 출처에서 dex 파일, 네이티브 코드와 같이 실행 가능한 코드를 다운로드하는 앱 또는 서드 파티 코드(예: SDK)
- 사용자의 사전 동의 없이 기기에 다른 앱을 설치하는 앱
- 악성 소프트웨어 배포 또는 설치로 연결하거나 이러한 활동을 조장하는 앱
- 신뢰할 수 없는 웹 콘텐츠(예: http:// URL) 또는 신뢰할 수 없는 출처에서 획득한 확인되지 않은 URL(예: 신뢰할 수 없는 인텐트를 통해 획득한 URL)을 로드하는 JavaScript 인터페이스가 추가된 웹뷰 포함 앱 또는 서드 파티 코드(예: SDK)
- 전체 화면 인텐트 권한 을 이용하여 불편을 야기하는 광고 또는 알림을 통해 사용자가 상호작용하도록 강제하는 앱

포그라운드 서비스 사용

포그라운드 서비스 권한은 사용자 대상 포그라운드 서비스가 적절히 작동하는 데 필요합니다. Android 14 이상을 타겟팅하는 앱의 경우 앱에 사용되는 포그라운드 서비스마다 유효한 포그라운드 서비스 유형을 지정하고 해당 유형에 적합한 포그라운드 서비스 권한을 선언해야 합니다. 예를 들어 앱의 사용 사례에서 지도 위치정보가 필요한 경우 앱의 매니페스트에서 FOREGROUND_SERVICE_LOCATION 권한을 선언해야 합니다.

앱은 다음과 같은 경우에만 포그라운드 서비스 권한을 선언할 수 있습니다.

- 사용자에게 유용하며 앱의 핵심 기능과 관련이 있는 기능을 제공함
- 포그라운드 서비스 사용을 사용자가 시작함 또는 사용자가 인식할 수 있음(예: 노래 재생 소리, 다른 기기에 미디어 전송, 정확하고 명확한 사용자 알림, 사진을 클라우드에 업로드하기 위한 사용자 요청).
- 사용자가 포그라운드 서비스 사용을 종료하거나 중단할 수 있음
- 부정적인 사용자 경험 또는 사용자가 예상한 기능의 오작동을 초래하는 경우를 제외하고 시스템에 의해 중단 또는 지연되어서는 안 됨(예: 전화 통화는 즉시 시작되어야 하고 시스템에 의해 지연되어서는 안 됨)
- 작업을 완료하기 위해 필요할 때만 권한이 실행됨

다음 포그라운드 서비스 사용 사례는 위의 기준에서 제외됩니다.

- 포그라운드 서비스 유형 systemExempted 또는 shortService
- 포그라운드 서비스 유형 dataSync, Play Asset Delivery 기능을 사용하는 경우에만 해당

포그라운드 서비스 사용에 관한 자세한 내용은 여기를 참고하세요.

사용자가 개시한 데이터 전송 작업

앱에서는 다음과 같이 사용하는 경우에만 사용자가 시작한 데이터 전송 작업 API를 사용할 수 있습니다.

- 사용자가 사용을 시작함

- 네트워크 데이터 전송 작업 용도
- 데이터 전송을 완료하기 위해 필요한 시간 동안만 실행

User-Initiated Data Transfer API 사용에 관한 자세한 내용은 여기를 참고하세요.

Flag_Secure 관련 요구사항

FLAG_SECURE 는 앱의 코드에 선언된 디스플레이 플래그로, 앱을 사용하는 동안 안전한 경로에서만 제한적으로 표시하고자 하는 민감한 데이터가 UI에 포함되어 있음을 나타냅니다. 이 플래그는 데이터가 스크린샷 또는 보안되지 않은 디스플레이에 표시되지 않도록 방지합니다. 앱 콘텐츠를 앱 또는 사용자 기기 외부로 브로드캐스트 또는 다른 방식으로 전송하거나 외부에서 이를 확인해서는 안 되는 경우 개발자는 이 플래그를 선언합니다.

보안 및 개인 정보 보호를 위해 Google Play에서 배포되는 모든 앱은 다른 앱의 FLAG_SECURE 선언을 존중해야 합니다. 즉, 앱은 다른 앱의 FLAG_SECURE 설정을 우회하도록 조장하거나 이를 위한 우회 수단을 만들어 내서는 안 됩니다.

접근성 도구 로 간주되는 앱은 사용자 기기 외부에서 액세스하기 위해 FLAG_SECURE로 보호되는 콘텐츠를 전송, 저장 또는 캐시하지 않는 한 이 요건에서 면제됩니다.

기기 전용 Android 컨테이너를 실행하는 앱

온디바이스 Android 컨테이너 앱은 기본 Android OS의 전부 또는 일부를 시뮬레이션하는 환경을 제공합니다. 이러한 환경 내 경험에 일부 Android 보안 기능 이 반영되지 않을 수 있습니다. 이에 따라 개발자는 시뮬레이션된 Android 환경에서 작동해서는 안 되는 온디바이스 Android 컨테이너와 통신할 수 있도록 보안 환경 매니페스트 플래그를 추가할 수 있습니다.

보안 환경 매니페스트 플래그

REQUIRE_SECURE_ENV 는 특정 앱의 매니페스트에서 선언하여 이 앱을 온디바이스 Android 컨테이너 앱에서 실행해서는 안 된다는 점을 나타낼 수 있는 플래그입니다. 보안 및 개인 정보 보호를 위해 온디바이스 Android 컨테이너를 제공하는 앱은 이 플래그 및 다음을 선언하는 모든 앱을 존중해야 합니다.

- 온디바이스 Android 컨테이너에서 이 플래그에 대해 로드하고자 하는 앱의 매니페스트를 검토합니다.
- 이 플래그를 선언한 앱을 온디바이스 Android 컨테이너에 로드하지 않습니다.
- 컨테이너에 설치되는 것처럼 보이도록 기기에서 API를 가로채거나 호출함으로써 프록시로 작동하지 않습니다.
- 플래그를 우회하기 위한 해결책(예: 이전 버전의 앱을 로드하여 현재 앱의 REQUIRE_SECURE_ENV 플래그 우회)을 조장하거나 만들지 않습니다.

고객센터에서 해당 정책을 자세히 알아보세요.

사기 행위

앱이 사용자를 속이려고 시도하거나 부정행위를 조장해서는 안 됩니다. 여기에는 기능적으로 불가능하도록 제작된 앱을 포함하되 이에 국한되지 않습니다. 앱은 메타데이터의 모든 부분에서 앱의 기능을 정확하게 공개하고 설명하며, 기능에 관한 이미지/동영상을 제공해야 합니다. 앱이 운영체제나 다른 앱의 기능 또는 경고를 모방하려고 해서는 안 됩니다. 기기 설정을 변경하려면 사용자에게 알린 후 동의를 받아야 하며, 변경된 설정을 사용자가 되돌릴 수 있어야 합니다.

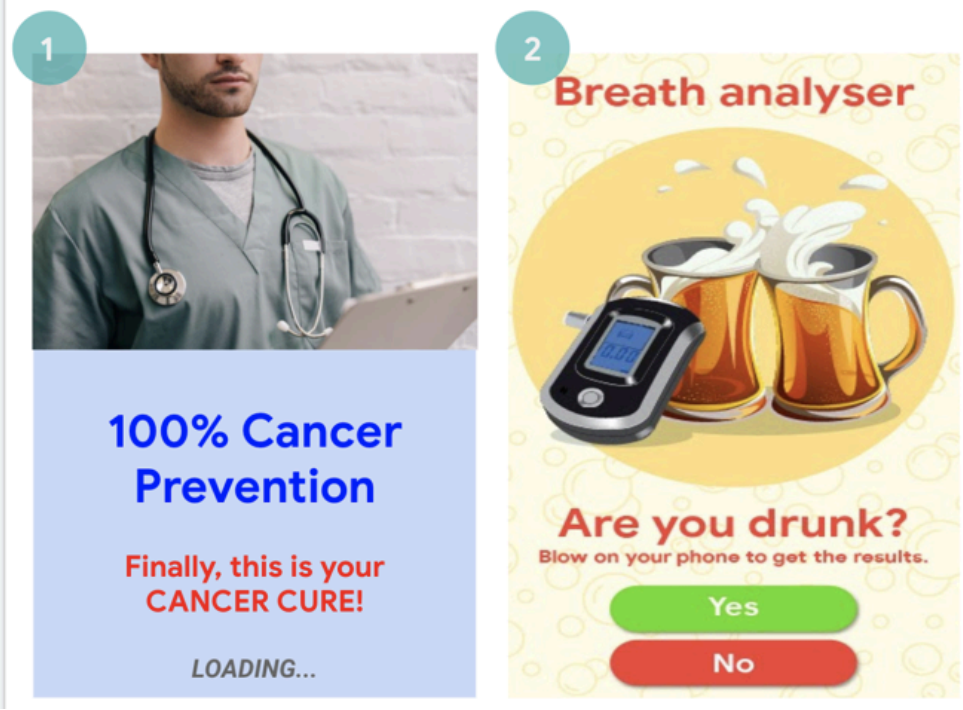
왜곡된 주장

설명, 제목, 아이콘, 스크린샷 등에 잘못되거나 오해의 소지가 있는 정보 또는 주장이 포함된 앱은 허용되지 않습니다.

다음은 자주 발생하는 위반 사례입니다.

- 앱이 기능을 허위로 진술하거나 정확하고 명확하게 설명하지 않습니다.
  - 앱이 설명과 스크린샷에서 레이싱 게임이라고 주장하지만, 실제로는 자동차 사진을 사용한 퍼즐 블록 게임입니다.

  - 앱이 바이러스 백신 앱이라고 주장하지만, 실제로는 바이러스를 제거하는 방법을 설명하는 텍스트 안내로만 이뤄져 있습니다.
- 장난, 가짜, 농담 등으로 표시되어 있더라도 해충 방지 앱과 같이 앱이 실제로는 구현할 수 없는 기능을 제공한다고 주장합니다.
- 앱이 부적절하게 분류되었습니다. 여기에는 앱 평점 또는 앱 카테고리가 포함되지만 이에 국한되지 않습니다.
- 투표 절차를 방해할 수 있는, 또는 선거 결과에 관한 명백한 사기성 또는 허위 콘텐츠입니다.
- 앱이 정부 기관과 제휴되어 있다고 허위로 주장하거나, 적절한 허가를 받지 못했음에도 불구하고 정부 서비스를 제공 또는 지원한다고 허위로 주장합니다.
- 허위로 기존 법인의 공식 앱을 사칭하는 앱입니다. 필요한 허가 또는 권리 없이 '저스틴 비버 공식 앱'과 같은 제목을 사용할 수 없습니다.



(1) 이 앱에는 오해를 불러일으키는 의료 또는 건강 관련 주장(암 치료)이 담겨 있습니다.
(2) 이 앱은 구현할 수 없는 기능(휴대전화를 음주 측정기로 사용)을 제공한다고 주장합니다.

사기성 기기 설정 변경

사용자에게 알려 동의를 받지 않은 상태로 앱 외부의 사용자 기기 설정 또는 기능을 변경하는 앱은 허용되지 않습니다. 기기의 설정 및 기능에는 시스템 및 브라우저 설정, 북마크, 바로가기, 아이콘, 위젯, 메인 스크린의 앱 표시 방법 등이 포함됩니다.

또한 다음과 같은 사항이 허용되지 않습니다.

- 사용자의 동의를 받았지만 손쉽게 되돌릴 수 없는 방식으로 기기 설정 또는 기능을 변경하는 앱
- 제3자에게 서비스를 제공하거나 광고 목적으로 기기 설정 또는 기능을 변경한 앱 또는 광고
- 사용자가 타사 앱을 삭제 또는 사용 중지하거나 기기 설정 또는 기능을 변경하도록 호도하는 앱
- 확인 가능한 보안 서비스가 아닌데 사용자가 타사 앱을 삭제 또는 사용 중지하거나 기기 설정 또는 기능을 변경하도록 조장하거나 이러한 활동에 인센티브를 지급하는 앱

부정행위 조장

사용자가 타인을 속이는 데 일조하거나 어떠한 방식으로든 사기성 기능이 있는 앱은 허용되지 않습니다. 여기에는 신분증, 주민등록번호, 여권, 졸업 증명서, 신용카드, 은행 계좌, 운전면허증을 위조하거나 이러한 활동을 돕는 앱이 포함되지만 이에 국한되지 않습니다. 앱은 앱의 기능 및/또는 콘텐츠와 관련된 공개사항, 제목, 설명, 이미지/동영상을 정확하게 제공해야 하며 사용자가 합리적으로 예측할 수 있는 방식으로 작동해야 합니다.

추가 앱 리소스(예: 게임 애셋)는 사용자가 앱을 사용하다가 필요할 때만 다운로드할 수 있어야 합니다. 다운로드된 리소스는 모든 Google Play 정책을 준수해야 하며, 다운로드가 시작되기 전에 앱에서 사용자에게 메시지를 표시하고 다운로드 크기를 명확하게 공개해야 합니다.

앱이 '장난', '재미 목적'(또는 이와 비슷한 표현)이라고 주장하는 경우에도 Google 정책이 적용됩니다.

다음은 자주 발생하는 위반 사례입니다.

- 다른 앱 또는 웹사이트를 모방하여 개인 정보나 인증 정보를 공개하도록 속이는 앱
- 개인 또는 법인의 동의 없이 확인되지 않았거나 실제로 존재하는 전화번호, 연락처, 주소 또는 개인 식별 정보를 표시하는 앱
- 사용자 지역, 기기 매개변수 또는 기타 사용자별 데이터에 따라 핵심 기능의 차이가 있음에도 스토어 등록정보에서 이러한 차이를 사용자의 눈에 띄게 공지하지 않은 앱
- 사용자에게 알림을 보내거나(예: '새로운 기능' 섹션) 스토어 등록정보를 업데이트하지 않은 상태에서 버전 간 대대적인 변화가 이루어지는 앱
- 검토 중 행동을 수정하거나 난독화하려고 시도하는 앱
- 다운로드 전에 사용자에게 알림을 표시하지 않고 크기가 공개되지 않은 다운로드를 콘텐츠 전송 네트워크(CDN)를 통해 처리하는 앱

조작된 미디어

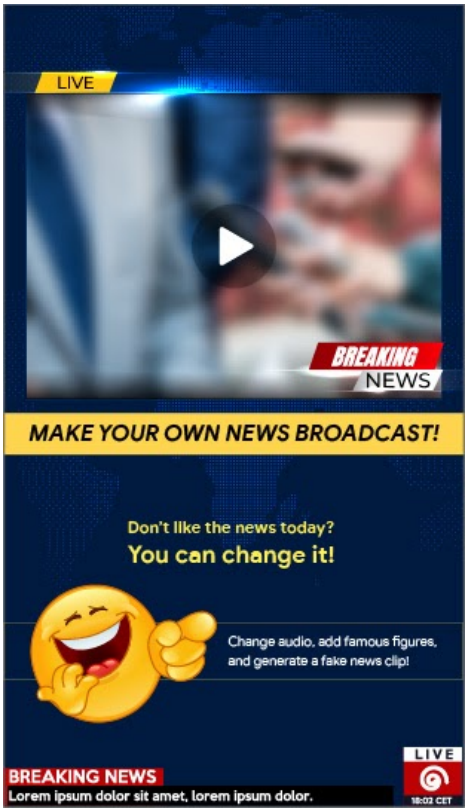
이미지, 오디오, 동영상 및/또는 텍스트를 통해 전달되며 잘못되거나 혼동을 야기하는 정보 또는 주장을 조장하거나 만들어 내는 앱은 허용되지 않습니다. 명백하게 혼동을 야기하거나 사기성이 있는 이미지, 동영상 및/또는 텍스트를 조장하거나 끊임없이 반복하는 것으로 확인된 앱은 민감한 사건, 정치, 사회적 문제 또는 기타 공적 관심사의 문제와 관련해 피해를 유발할 수 있으므로 허용되지 않습니다.

공익에 부합하거나, 명백히 인공적인 이미지이거나, 사용자 대상 고지 또는 워터마크를 포함하는 조작된 미디어이거나, 명백한 풍자 또는 패러디인 경우에는 예외가 적용될 수 있습니다.

조작된 미디어는 제한된 콘텐츠 정책에 따라 허용되지 않는 콘텐츠 금지 등 기존 Google Play 개발자 정책을 준수해야 합니다.

다음은 자주 발생하는 위반 사례입니다.

- 앱이 스토어 등록정보에서 민감한 사건의 유명 인사 또는 미디어를 사용하여 미디어 변경 기능을 광고합니다.
- 앱이 명확한 고지나 워터마크 없이 실제 언론사의 이름 또는 로고를 포함하여 미디어 클립을 뉴스 보도인 것처럼 변경합니다.
- 앱의 유일한 목적이 허위 정보 또는 혼동을 야기하는 미디어를 만드는 것입니다.



(1) 이 앱은 미디어 클립을 뉴스 보도인 것처럼 변경하고 워터마크 없이 클립에 유명 인사 또는 공인을 추가하는 기능을 제공합니다.

동작의 투명성

앱의 기능은 사용자에게 충분히 명확하게 전달되어야 하며, 숨겨진 기능, 비활성 기능 또는 문서화되지 않은 기능이 앱에 포함되어서는 안 됩니다. 앱 리뷰를 회피하는 기법은 허용되지 않습니다. 사용자의 안전, 시스템 무결성, 정책 준수를 보장하기 위해 앱에 관한 추가적인 세부정보를 제공해야 할 수도 있습니다.

허위 진술

다음과 같은 앱 또는 개발자 계정은 허용되지 않습니다.

- 개인 또는 조직의 명의를 도용하거나, 소유권 또는 주요 목적을 허위로 표시하거나 은폐합니다.
- 사용자를 오도하기 위해 조직된 활동에 관여합니다. 여기에는 앱이 기반을 둔 국가를 왜곡 또는 은폐하거나 다른 국가의 사용자를 대상으로 콘텐츠를 제공하는 앱 또는 개발자 계정을 포함하되 이에 국한되지 않습니다.
- 앱 콘텐츠가 정치, 사회 문제 또는 공적인 사안과 관련된 경우 다른 앱, 사이트, 개발자 또는 기타 계정과 협력하여 개발자나 앱 ID 또는 기타 중요 세부정보를 은폐하거나 허위 표시합니다.

Google Play의 대상 API 수준 정책

사용자에게 안전하고 보안이 유지되는 환경을 제공하기 위해 Google Play에서는 **모든 앱**에 다음과 같은 대상 API 수준을 요구합니다.

신규 앱과 앱 업데이트는 반드시 최신 Android 주 버전 출시로부터 1년 이내의 Android API 수준을 타겟팅해야 합니다. 이 요건을 충족하지 못하는 신규 앱과 앱 업데이트는 Play Console에서 앱 제출이 허용되지 않습니다.

최신 Android 주 버전 출시로부터 2년 이내의 API 수준을 타겟팅하지 않고 **업데이트도 되지 않은 기존 Google Play 앱**은 상위 버전의 Android OS 실행 기기를 사용하는 신규 사용자에게 제공되지 않습니다. 이전에 Google Play에서 앱을 설치했던 사용자는 앞으로도 해당 앱이 지원하는 Android OS 버전에서 앱을 계속 탐색, 재설치, 사용할 수 있습니다.

대상 API 수준 요구사항을 충족하는 방법에 관한 기술적 조언은 이전 가이드 를 참고하세요.

정확한 타임라인 및 예외사항은 이 고객센터 문서 를 참고하세요.

사용자 데이터 정책

사용자 데이터(예: 기기 정보를 포함하여 사용자로부터 수집하거나 사용자에 관해 수집한 정보)를 투명하게 처리해야 합니다. 이는 앱 사용자 데이터의 액세스, 수집, 사용, 처리, 공유에 관해 공개하고 데이터의 용도를 공개된 정책상 목적으로 제한한다는 의미입니다.

앱에 SDK와 같은 서드 파티 코드가 포함되는 경우 앱에 사용된 서드 파티 코드와 앱의 사용자 데이터와 관련된 해당 서드 파티의 관행이 Google Play 개발자 프로그램 정책을 준수하는지 확인해야 하며, 여기에는 사용 및 공개 요건이 포함됩니다. 예를 들어 SDK 제공업체가 앱의 개인 정보 및 민감한 사용자 데이터를 판매하지 않는지 확인해야 합니다. 이 요건은 사용자 데이터가 서버로 전송된 후 이전되는지 또는 앱에 서드 파티 코드를 삽입하는 방식인지 여부와 관계없이 적용됩니다.

개인 정보 및 민감한 사용자 데이터

- 앱을 통해 획득한 개인 정보 및 민감한 사용자 데이터의 액세스, 수집, 사용, 공유는 사용자가 합리적으로 예상하는 앱 및 서비스 기능과 정책에 부합하는 목적으로 제한됩니다.
  - 광고 게재를 위해 개인 정보 및 민감한 사용자 데이터의 사용을 확장하는 앱은 Google Play의 광고 정책을 준수해야 합니다.
- 전송에 최신 암호화 기술(예: HTTPS 연결)을 사용하는 등 모든 개인 정보 및 민감한 사용자 데이터를 안전하게 처리합니다.
- 가능한 경우 Android 권한을 통해 관리되는 데이터에 액세스하기 전에 런타임 권한 요청을 사용합니다.

개인 정보 및 민감한 사용자 데이터의 판매

개인 정보 및 민감한 사용자 데이터를 판매하지 않습니다.

- '판매'란 개인 정보 및 민감한 사용자 데이터를 금전적인 대가를 받고 교환하거나 제3자에게 전송하는 행위를 의미합니다.
  - 사용자가 개시한 개인 정보 및 민감한 사용자 데이터의 전송(예: 사용자가 앱의 기능을 사용해 제3자에게 파일을 전송하는 경우 또는 사용자가 조사 연구를 목적으로 하는 앱을 사용하기로 선택하는 경우)은 판매로 간주되지 않습니다.

명시적 공개 및 동의 요건

앱의 개인 정보 및 민감한 사용자 데이터 액세스, 수집, 사용 또는 공유가 해당 제품 또는 기능을 사용하는 사용자의 합리적인 기대 범위 내에 포함되지 않을 수 있는 경우 사용자 데이터 정책의 명시적 공개 및 동의 요건을 충족해야 합니다.

앱이 개인 정보 및 민감한 사용자 데이터를 기본적으로 수집하도록 만들어진 서드 파티 코드(예: SDK)를 통합하는 경우 Google Play에서 요청을 받은 후 2주 이내에(또는 Google Play가 요청에서 더 긴 기간을 제공한 경우 해당 기간 내에), 서드 파티 코드를 통한 데이터 액세스, 수집, 사용 또는 공유 관련 요건을 비롯하여 앱이 본 정책의 명시적 공개 및 동의 요건을 준수한다는 사실을 보여주는 충분한 증거를 제공해야 합니다.

SDK 등의 서드 파티 코드 사용으로 인해 앱이 사용자 데이터 정책을 위반하지 않도록 해야 합니다.

명시적 공개 및 동의 요건에 관한 자세한 내용은 이 고객센터 도움말을 참고하세요.

SDK로 인한 위반의 예

- 앱이 SDK를 통해 개인 정보 및 민감한 사용자 데이터를 수집하지만 이러한 데이터를 이 사용자 데이터 정책, 액세스, 데이터 처리(허용되지 않는 판매 포함), 명시적 공개 및 동의 요건의 대상으로 취급하지 않습니다.
- 앱에 통합된 SDK가 기본적으로 개인 정보 및 민감한 사용자 데이터를 수집하면서 이 정책의 사용자 동의 및 명시적 공개에 관한 요건을 위반합니다.
- 앱에 사용된 SDK가 앱에서 사기 및 악용 방지 기능을 제공할 목적으로만 개인 정보 및 민감한 사용자 데이터를 수집한다고 주장하지만 SDK에서 수집한 데이터가 광고 또는 분석을 위해 서드 파티와 공유됩니다.
- 명시적 공개 가이드라인 및/또는 개인정보처리방침 가이드라인을 준수하지 않고 사용자가 설치한 패키지 정보를 전송하는 SDK가 앱에 포함되어 있습니다.
  - 원치 않는 모바일 소프트웨어 정책도 참고하세요.

개인 정보 및 민감한 정보 액세스에 관한 추가 요구사항

아래 표에는 특정 활동에 관한 요구사항이 설명되어 있습니다.

활동	요구사항
앱이 영구적인 기기 식별자를 수집 또는 연결하는 경우(예: IMEI, IMSI, SIM 일련번호)	영구적인 기기 식별자는 다음 용도를 제외하고는 다른 개인 정보 및 민감한 사용자 데이터 또는 재설정 가능한 기기 식별자와 연결할 수 없습니다.

	• SIM 아이덴티티와 연결된 전화 통신(예: 이동통신사 계정에 연결된 Wi-Fi 통화) • 기기 소유자 모드를 사용하는 기업 기기 관리 앱 이러한 용도는 사용자 데이터 정책에 명시된 대로 사용자에게 명확하게 공개되어야 합니다. 다른 고유 식별자에 관해 알아보려면 이 리소스를 참고 하세요. Android 광고 ID에 관한 추가 가이드라인은 광고 정책에서 확인하세요.
앱이 아동을 대상으로 하는 경우	앱에는 아동 대상 서비스에 사용할 수 있도록 자체 인증한 SDK만 포함할 수 있습니다. 정책 전문 및 요구사항은 가족용 자체 인증 광고 SDK 프로그램을 참고하세요.

SDK로 인한 위반의 예

- 앱에서 사용하는 SDK가 IMEI 및 위치를 연결합니다.
- 앱에서 사용하는 SDK가 Android 광고 ID(AAID)를 광고 또는 분석 목적으로 영구적인 기기 식별자에 연결합니다.
  앱에서 사용하는 SDK가 분석 목적으로 AAID 및 이메일 주소를 연결합니다.

데이터 보안 섹션

모든 개발자는 앱마다 사용자 데이터의 수집, 사용, 공유에 관한 자세한 설명을 포함하여 데이터 보안 섹션을 명확하고 정확하게 작성해야 합니다. 여기에는 앱에 사용된 서드 파티 라이브러리 또는 SDK를 통해 수집되고 처리되는 데이터가 포함됩니다. 개발자는 라벨을 정확히 작성하고 정보를 최신 상태로 유지할 책임이 있습니다. 해당하는 경우 데이터 보안 섹션은 앱의 개인정보처리방침에 공개된 내용과 일치해야 합니다.

데이터 보안 섹션 작성에 관한 추가 정보는 이 고객센터 도움말을 참고하세요.

사용자 데이터 정책 전문을 확인하세요.

민감한 정보에 액세스하는 권한 및 API 정책

민감한 정보 액세스 권한 및 API에 관한 요청은 사용자가 이해할 수 있어야 합니다. Google Play 등록정보에서 홍보된 앱의 현재 기능 또는 서비스를 구현하는 데 필요한 민감한 정보 액세스 권한 및 API만 요청할 수 있습니다. 공개, 구현 또는 허용되지 않은 기능이나 목적을 위해 사용자 또는 기기 데이터에 액세스하는 민감한 정보 액세스 권한 또는 API를 사용해서는 안 됩니다. 민감한 정보에 액세스하는 권한 또는 API를 통해 액세스한 개인 정보 또는 민감한 정보는 절대로 판매하거나 판매를 촉진할 목적으로 공유할 수 없습니다.

민감한 정보에 액세스하는 권한 및 API 정책 전문을 확인하세요.

SDK로 인한 위반의 예

- 앱에 포함된 SDK가 허용되지 않거나 공개되지 않은 목적으로 백그라운드에서 위치 정보를 요청합니다.
- 앱에 포함된 SDK가 사용자의 동의 없이 read_phone_state Android 권한에서 파생된 IMEI를 전송합니다.

멀웨어 정책

Google은 Google Play 스토어를 포함한 Android 생태계와 사용자 기기에는 악의적 행위(즉, 멀웨어)가 없어야 한다는 단순 명료한 멀웨어 정책을 견지합니다. 이 기본적인 원칙을 통해 사용자와 Android 기기를 위한 안전한 Android 생태계를 조성하고자 노력하고 있습니다.

멀웨어란 사용자, 사용자 데이터 또는 기기를 위험에 노출할 수 있는 모든 코드를 말합니다. 멀웨어는 잠재적으로 위험한 애플리케이션(PHA), 바이너리 또는 프레임워크 수정을 포함하되 이에 국한되지 않으며 트로이 목마, 피싱, 스파이웨어 앱과 같은 카테고리로 이루어집니다. Google은 지속적으로 새로운 카테고리를 업데이트 및 추가하고 있습니다.

이 정책의 요구사항은 앱에 포함된 모든 서드 파티 코드(예: SDK)에도 적용됩니다.

멀웨어 정책 전문을 확인하세요.

SDK로 인한 위반의 예

- 악성 소프트웨어를 배포하는 제공업체의 SDK 라이브러리가 앱에 포함되어 있습니다.
- 앱이 Android 권한 모델을 위반하거나 다른 앱에서 OAuth 토큰과 같은 사용자 인증 정보를 탈취합니다.
- 앱이 제거 또는 중단되지 않도록 기능을 악용합니다.
- 앱이 SELinux를 사용 중지합니다.
- 앱에 포함된 SDK가 공개되지 않은 목적으로 기기 데이터에 액세스하여 승격된 권한을 획득하는 방식으로 Android 권한 모델을 위반합니다.
- 휴대전화 요금 청구를 통해 콘텐츠를 구독하거나 구매하도록 사용자를 속이는 코드가 SDK와 함께 앱에 포함되어 있습니다.

앱에서의 SDK 사용

앱에 SDK를 포함할 경우 서드 파티 코드와 관행으로 인해 앱이 Google Play 개발자 프로그램 정책을 위반하지 않도록 할 책임은 개발자에게 있습니다. 앱의 SDK가 어떻게 사용자 데이터를 처리하는지 인지해야 하며, 어떤 권한을 사용하고 어떤 데이터를 수집하며 그 이유는 무엇인지를 파악해야 합니다.

SDK 요구사항

앱 개발자는 앱의 주요 기능과 서비스를 통합하기 위해 SDK와 같은 서드 파티 코드를 사용하는 경우가 많습니다. 앱에 SDK를 포함할 때는 모든 취약점으로부터 사용자와 앱을 안전하게 보호할 수 있어야 합니다. 이 섹션에서는 기존 개인 정보 보호 및 보안 요구사항 중 일부가 SDK 측면에서는 어떻게 적용되고, 개발자가 SDK를 앱에 안전하게 통합하는 데 어떻게 도움이 되는지를 살펴봅니다.

앱에 SDK를 포함할 경우 서드 파티 코드와 관행으로 인해 앱이 Google Play 개발자 프로그램 정책을 위반하지 않도록 할 책임은 개발자에게 있습니다. 앱의 SDK가 어떻게 사용자 데이터를 처리하는지 인지해야 하며, 어떤 권한을 사용하고 어떤 데이터를 수집하며 그 이유는 무엇인지를 파악해야 합니다. SDK는 앱의 정책상 사용자 데이터 활용 방식에 부합하도록 해당 데이터를 수집하고 처리해야 합니다.

SDK 사용 시 정책 요구사항을 위반하지 않으려면 아래에 있는 다음 정책을 전체적으로 읽고 이해한 후 기존 요구사항 중 SDK와 관련된 내용을 참고하시기 바랍니다.

사용자 권한 없이 기기를 루팅하는 권한 에스컬레이션 앱은 루팅 앱으로 분류됩니다.

스파이웨어

스파이웨어는 정책 준수 기능과 관련 없는 사용자 또는 기기 데이터를 수집, 유출 또는 공유하는 악성 애플리케이션, 코드 또는 동작입니다.

사용자를 염탐하는 것으로 간주될 수 있거나 적절한 고지 또는 동의 없이 데이터를 유출하는 악성 코드 또는 동작도 스파이웨어로 간주됩니다.

스파이웨어 정책 전문을 참고하세요.

예를 들어 SDK로 인한 스파이웨어 위반은 다음을 포함하되 이에 국한되지 않습니다.

- 정책을 준수하는 앱 기능과 관련이 없는 경우 오디오 또는 통화 녹음의 데이터를 전송하는 SDK를 사용하는 앱
- 사용자가 예상하지 못한 방식 및/또는 적절한 사용자 고지 또는 동의 없이 데이터를 기기 밖으로 전송하는 악성 서드 파티 코드(예: SDK)가 포함된 앱

원치 않는 모바일 소프트웨어 정책

투명한 행동과 명확한 공개

모든 코드는 사용자에게 약속한 내용을 전달해야 합니다. 앱은 안내한 모든 기능을 제공해야 하며 사용자의 혼란을 유도하지 않아야 합니다.

위반 예시:

- 광고 사기
- 소셜 엔지니어링

사용자 데이터 보호

개인 정보 및 민감한 사용자 데이터의 액세스, 사용, 수집, 공유에 관해 명확하고 투명하게 공개합니다. 사용자 데이터 사용 시에는 적용되는 모든 관련 사용자 데이터 정책을 준수하고 데이터 보호를 위한 모든 예방 조치를 취해야 합니다.

위반 예시:

- 데이터 수집(스파이웨어 참고)
- 제한된 권한 악용

원치 않는 모바일 소프트웨어 정책 전문을 확인하세요.

기기 및 네트워크 악용 정책

사용자의 기기, 기타 기기 또는 컴퓨터, 서버, 네트워크, 애플리케이션 프로그래밍 인터페이스(API), 서비스(기기에 설치된 기타 앱, Google 서비스, 승인된 이동통신사 네트워크를 포함하되 이에 국한되지 않음)를 방해하거나, 작동에 지장을 주거나, 손상하거나, 무단으로 액세스하는 앱은 허용되지 않습니다.

런타임에 로드되는(예: 앱에 패키징되지 않음) 인터프리트 언어(자바스크립트, Python, Lua 등)가 포함된 앱 또는 서드 파티 코드(예: SDK)에서 잠재적인 Google Play 정책 위반을 허용해서는 안 됩니다.

보안 취약점을 야기하거나 악용하는 코드는 허용되지 않습니다. 개발자에게 신고된 최근 보안 문제에 관해 알아보려면 앱 보안 개선 프로그램을 확인하세요.

기기 및 네트워크 악용 정책 전문을 확인하세요.

SDK로 인한 위반의 예

- 서드 파티에 프록시 서비스를 제공하는 앱은 사용자를 대상으로 이러한 기능을 제공하는 것이 앱의 주된 목적인 경우에만 서비스를 제공할 수 있습니다.
- dex 파일, 네이티브 코드 등 Google Play 외 소스의 실행 코드를 다운로드하는 SDK가 앱에 포함되어 있습니다.
- WebView를 포함하는 SDK가 앱에 포함되어 있으며, 이 WebView에는 신뢰할 수 없는 웹 콘텐츠(예: http:// URL) 또는 신뢰할 수 없는 출처에서 획득한 확인되지 않은 URL(예: 신뢰할 수 없는 인텐트를 통해 획득한 URL)을 로드하는 JavaScript 인터페이스가 추가되어 있습니다.
- 자체 APK를 업데이트하는 데 사용하는 코드가 포함된 SDK가 앱에 포함되어 있습니다.
- 비보안 연결을 통해 파일을 다운로드하여 사용자를 보안 취약점에 노출시키는 SDK가 앱에 포함되어 있습니다.
- 앱이 Google Play 외부의 알 수 없는 소스에서 애플리케이션을 다운로드하거나 설치하는 코드가 포함된 SDK를 사용합니다.
- 적절한 사용 사례 없이 포그라운드 서비스를 사용하는 SDK가 앱에 포함되어 있습니다.
- 정책 준수를 위해 포그라운드 서비스를 사용하는 SDK가 앱에 포함되어 있지만, 포그라운드 서비스를 사용한다는 사실이 앱 매니페스트에 선언되어 있지 않습니다.

사기 행위 정책

앱이 사용자를 속이려고 시도하거나 부정행위를 조장해서는 안 됩니다. 여기에는 기능적으로 불가능하도록 제작된 앱을 포함하되 이에 국한되지 않습니다. 앱은 메타데이터의 모든 부분에서 앱의 기능을 정확하게 공개하고 설명하며, 기능에 관한 이미지/동영상을 제공해야 합니다. 앱이 운영체제나 다른 앱의 기능 또는 경고를 모방하려고 해서는 안 됩니다. 기기 설정을 변경하려면 사용자에게 알린 후 동의를 받아야 하며, 변경된 설정을 사용자가 되돌릴 수 있어야 합니다.

전체 사기 행위 정책을 확인하세요.

동작의 투명성

앱의 기능은 사용자에게 충분히 명확하게 전달되어야 하며, 숨겨진 기능, 비활성 기능 또는 문서화되지 않은 기능이 앱에 포함되어서는 안 됩니다. 앱 리뷰를 회피하는 기법은 허용되지 않습니다. 사용자의 안전, 시스템 무결성, 정책 준수를 보장하기 위해 앱에 관한 추가적인 세부정보를 제공해야 할 수도 있습니다.

SDK로 인한 위반의 예

- 앱에 앱 리뷰를 회피하는 기법을 사용하는 SDK가 포함되어 있습니다.

일반적으로 어떤 Google Play 개발자 정책이 SDK로 인한 위반과 관련되어 있나요?

앱에서 사용하는 모든 서드 파티 코드가 Google Play의 개발자 프로그램 정책을 준수하도록 하려면 다음 정책을 전부 참고하시기 바랍니다.

- 사용자 데이터 정책
- 민감한 정보에 액세스하는 권한 및 API
- 기기 및 네트워크 악용 정책
- 멀웨어
- 원치 않는 모바일 소프트웨어
- 가족용 자체 인증 광고 SDK 프로그램
- 광고 정책
- 사기 행위
- Google Play 개발자 프로그램 정책

이러한 정책과 관련해 문제가 발생하는 경우가 더 일반적이기는 하지만 부적합한 SDK 코드로 인해 앱이 위에 참조되지 않은 다른 정책을 위반할 수도 있다는 점에 주의해야 합니다. SDK가 정책을 준수하는 방식으로 앱 데이터를 처리하도록 하는 것은 앱 개발자의 책임이므로 모든 정책을 전부 검토하고 최신 정보를 알아두시기 바랍니다.

자세한 내용은 고객센터를 참고하세요.

멀웨어

Google은 Google Play 스토어를 포함한 Android 생태계와 사용자 기기에는 악의적 행위(즉, 멀웨어)가 없어야 한다는 단순 명료한 멀웨어 정책을 견지합니다. 이 기본적인 원칙을 통해 사용자와 Android 기기를 위한 안전한 Android 생태계를 조성하고자 노력하고 있습니다.

멀웨어란 사용자, 사용자 데이터 또는 기기를 위험에 노출할 수 있는 모든 코드를 말합니다. 멀웨어는 잠재적으로 위험한 애플리케이션(PHA), 바이너리 또는 프레임워크 수정을 포함하되 이에 국한되지 않으며 트로이 목마, 피싱, 스파이웨어 앱과 같은 카테고리로 이루어집니다. Google은 지속적으로 새로운 카테고리를 업데이트 및 추가하고 있습니다.

이 정책의 요구사항은 앱에 포함된 모든 서드 파티 코드(예: SDK)에도 적용됩니다.

유형과 기능은 다양하지만 멀웨어의 목표는 보통 다음 중 하나입니다.

- 사용자 기기의 무결성을 저해합니다.
- 사용자 기기의 제어권을 획득합니다.
- 공격자가 원격 제어 작업을 통해 감염된 기기에 액세스하고 이를 활용하거나 다른 방식으로 악용하도록 합니다.
- 적절한 공개 또는 동의 없이 개인 정보 또는 사용자 인증 정보를 기기 밖으로 전송합니다.
- 감염된 기기에서 스팸 또는 명령어를 배포하여 다른 기기나 네트워크에 영향을 미칩니다.
- 사용자를 대상으로 사기를 저지릅니다.

앱, 바이너리 또는 프레임워크 수정은 잠재적으로 유해할 수 있으므로 해를 끼치려고 의도하지 않았더라도 악의적 행위를 유발할 수 있습니다. 이는 앱, 바이너리 또는 프레임워크 수정이 다양한 변수에 따라 다르게 기능하기 때문입니다. 따라서 하나의 Android 기기에 유해한 것이 다른 Android 기기에는 전혀 위험을 초래하지 않을 수 있습니다. 예를 들어 최신 버전의 Android를 실행하는 기기는 지원 중단된 API를 사용하여 악의적 동작을 수행하는 유해한 앱의 영향을 받지 않지만 이전 버전의 Android를 여전히 실행하는 기기는 위험에 취약할 수 있습니다. 앱, 바이너리 또는 프레임워크 수정이 일부 또는 모든 Android 기기와 사용자에게 명백한 위험을 초래할 경우 멀웨어 또는 PHA로 표시됩니다.

아래에 있는 멀웨어 카테고리에는 사용자가 기기의 사용 방식을 파악하고, 강력한 혁신과 신뢰할 수 있는 사용자 환경을 지원하는 안전한 생태계를 촉진해야 한다는 Google의 기본적인 신념이 반영되어 있습니다.

자세한 내용은 Google Play 프로텍트 를 참고하세요.

백도어

잠재적으로 유해하고 원격으로 제어되며 원치 않는 작업을 기기에서 실행하도록 허용하는 코드입니다.

이러한 작업에는 앱, 바이너리 또는 프레임워크 수정이 자동으로 실행될 경우 이를 다른 멀웨어 카테고리 중 하나에 배치하는 동작이 포함될 수 있습니다. 일반적으로 백도어는 잠재적으로 유해한 작업이 기기에서 어떻게 발생할 수 있는지에 관한 설명이므로 청구 사기 또는 상용 스파이웨어와 같은 카테고리와 완전히 일치하지는 않습니다. 그 결과, 일부 상황에서는 백도어의 하위 집합이 Google Play 프로텍트에서 취약점으로 취급되기도 합니다.

결제 사기

의도적인 속임수로 사용자에게 자동 청구를 발생시키는 코드입니다.

모바일 결제 사기는 SMS 사기, 전화 사기, 과금 사기로 나뉩니다.

SMS 사기
동의 없이 사용자에게 프리미엄 SMS 전송 요금을 부과하거나, 공개 계약 또는 요금 부과 사실을 알리거나 정기 결제를 확인하는 이동통신사의 SMS 메시지를 숨겨 SMS 활동을 위장하려고 시도하는 코드입니다.

일부 코드는 SMS 전송 동작을 기술적으로 공개하더라도 SMS 사기를 가능하게 하는 추가 동작을 적용합니다. 예를 들어 공개 계약의 일부를 사용자로부터 숨기거나 읽을 수 없게 만들거나, 사용자에게 요금 부과 사실을 알리거나 정기 결제를 확인하는 이동통신사의 SMS 메시지를 조건부로 차단하는 경우가 있습니다.

전화 사기
사용자의 동의 없이 프리미엄 번호로 전화를 걸어 요금을 부과하는 코드입니다.

과금 사기
휴대전화 청구를 통해 콘텐츠를 정기 결제하거나 구매하도록 사용자를 속이는 코드입니다.

과금 사기에는 프리미엄 SMS와 프리미엄 통화를 제외한 모든 유형의 청구가 포함됩니다. 이러한 사기의 예로는 이동통신사 직접 결제, 무선 액세스 포인트(WAP), 모바일 선불요금 이체 등이 있습니다. WAP 사기는 과금 사기 중 가장 빈번하게 발생하는 유형입니다. WAP 사기에는 자동으로 로드되는 투명한 WebView에서 버튼을 클릭하도록 사용자를 속이는 행위가 포함될 수 있습니다. 작업을 실행하면 반복되는 정기 결제가 시작되고, 사용자가 금융 거래 사실을 알아채지 못하도록 확인 SMS 또는 이메일을 가로채는 경우가 많습니다.

스토커웨어

모니터링 목적으로 기기에서 개인 정보 또는 민감한 사용자 데이터를 수집하여 서드 파티(기업 또는 다른 개인)에게 전송하는 코드.

앱은 적절한 명시적 공개를 제공하고 사용자 데이터 정책 에서 요구하는 동의를 얻어야 합니다.

애플리케이션 모니터링 가이드라인

부모가 자녀를 모니터링하거나 기업 경영진이 개인 직원을 모니터링하는 등 오직 다른 개인을 모니터링할 목적으로 설계 및 마케팅되는 앱이 모니터링 앱으로 허용되려면 아래 설명된 요건을 모두 준수해야 합니다. 이러한 앱은 모니터링 대상자(예: 배우자)가 모니터링 사실을 인지하고 허가했더라도 지속적인 알림 표시 여부와 관계없이 타인을 추적하는 데 사용할 수 없습니다. 앱에서 매니페스트 파일에 IsMonitoringTool 메타데이터 플래그를 사용하여 모니터링 앱임을 정확히 선언해야 합니다.

모니터링 앱은 다음 요건을 준수해야 합니다.

- 앱을 감시 또는 비밀 사찰 솔루션으로 표시해서는 안 됩니다.
- 앱이 추적 동작을 숨기거나 클로킹해서는 안 되며 이 기능과 관련하여 사용자를 오도하려고 시도해서는 안 됩니다.
- 앱이 실행되는 동안 항상 사용자에게 지속적인 알림을 표시하고 앱을 명확하게 식별하는 고유한 아이콘을 표시해야 합니다.
- Google Play 스토어의 앱 설명에 모니터링 또는 추적 기능을 공개해야 합니다.
- Google Play에 등록된 앱과 앱 등록정보는 본 약관을 위반하는 기능(예: Google Play 외부에서 호스팅하는 정책 미준수 APK에 연결)을 활성화하거나 이러한 기능에 액세스하는 수단을 제공해서는 안 됩니다.

- 모든 관련 법규를 준수해야 합니다. 타겟팅 지역에서 앱이 합법적인지 판단할 책임은 전적으로 개발자에게 있습니다.

자세한 정보는 isMonitoringTool 플래그 사용 고객 센터 자료를 참고하세요.

서비스 거부(DoS)

사용자가 모르는 사이에 서비스 거부(DoS) 공격을 실행하거나, 다른 시스템과 리소스를 상대로 하는 분산 DoS 공격의 일부인 코드입니다.

예를 들어, 대량의 HTTP 요청을 전송하여 원격 서버에 과도한 부하를 유발하는 방법으로 발생할 수 있습니다.

적대적인 다운로더

그 자체가 잠재적으로 유해하지는 않지만 다른 PHA를 다운로드하는 코드입니다.

다음 중 하나에 해당할 경우 코드가 적대적인 다운로더일 수 있습니다.

- PHA를 퍼뜨리기 위해 만들어졌다고 믿을 만한 근거가 있으며, PHA를 다운로드했거나 앱을 다운로드하고 설치할 수 있는 코드가 포함된 경우
- 확인된 앱 다운로드 최소 기준값 500건 중 다운로드된 앱의 5% 이상이 PHA인 경우(25건의 확인된 PHA 다운로드).

주요 브라우저와 파일 공유 앱은 다음에 모두 해당할 경우 적대적 다운로더로 간주하지 않습니다.

- 사용자 상호작용 없이 다운로드를 유도하지 않는 경우
- 모든 PHA 다운로드가 사용자의 동의에 따라 시작되는 경우

Android 이외의 위협

Android 이외의 위협이 포함된 코드입니다.

이 앱은 Android 사용자 또는 기기에 해를 입힐 수는 없지만 다른 플랫폼에 유해할 수 있는 구성요소를 포함하고 있습니다.

피싱

신뢰할 수 있는 소스에서 가져온 것으로 위장하고 사용자의 인증 정보 또는 결제 정보를 요청하며 데이터를 제3자에게 전송하는 코드입니다. 이 카테고리는 이동 중인 사용자 인증 정보의 전송을 가로채는 코드에도 적용됩니다.

피싱의 일반적인 대상으로는 뱅킹 인증 정보, 신용카드 번호, 소셜 네트워크와 게임의 온라인 계정 인증 정보가 있습니다.

승격된 권한 악용

앱 샌드박스를 깨고 승격된 권한을 취득하거나 보안 관련 핵심 기능의 액세스 권한을 변경 또는 사용중지하여 시스템의 무결성을 손상시키는 코드입니다.

예

- 앱이 Android 권한 모델을 위반하거나 다른 앱에서 OAuth 토큰과 같은 사용자 인증 정보를 탈취합니다.
- 앱이 제거 또는 중단되지 않도록 기능을 악용합니다.
- 앱이 SELinux를 사용중지합니다.

사용자 허가 없이 기기를 루팅하는 권한 에스컬레이션 앱은 루팅 앱으로 분류됩니다.

랜섬웨어

기기 또는 기기의 데이터를 부분적으로 또는 포괄적으로 제어하고, 결제를 하거나 제어를 해제하는 조치를 취하도록 사용자에게 요구하는 코드입니다.

일부 랜섬웨어는 기기 데이터를 암호화한 다음 데이터를 복호화하거나 일반적인 사용자가 삭제할 수 없도록 기기 관리 기능을 활용하기 위해서는 결제를 하도록 요구합니다. 예

- 사용자가 기기의 잠금을 해제할 수 없도록 한 다음 사용자 제어 복원을 대가로 돈을 요구합니다.
- 기기의 데이터를 암호화하고 표면적으로는 데이터 복호화를 위해 결제를 요구합니다.
- 기기 정책 관리자 기능을 활용하고 사용자의 삭제를 차단합니다.

기기 관리 보조를 주된 목적으로 하는 기기를 통해 배포된 코드는 보안 잠금 및 관리 요구사항, 적절한 사용자 공개 및 동의 요구사항을 충족할 경우 랜섬웨어 카테고리에서 제외될 수 있습니다.

루팅

기기를 루팅하는 코드입니다.

비악성 루팅 코드와 악성 루팅 코드는 서로 다릅니다. 예를 들어 비악성 루팅 앱은 기기를 루팅한다는 사실을 사용자에게 알리고, 다른 PHA 카테고리에 적용되는 기타 잠재적 유해 작업은 실행하지 않습니다.

반면 악성 루팅 앱은 기기를 루팅한다는 사실을 사용자에게 알리지 않거나, 루팅에 관해 사전에 알리지만 다른 PHA 카테고리에 적용되는 기타 작업을 함께 실행합니다.

스팸

사용자 연락처에 메시지를 무단 전송하거나 기기를 이메일 스팸 중계기로 사용하는 코드입니다.

스파이웨어

스파이웨어는 정책 준수 기능과 관련 없는 사용자 또는 기기 데이터를 수집, 유출 또는 공유하는 악성 애플리케이션, 코드 또는 동작입니다.

사용자를 염탐하는 것으로 간주될 수 있거나 적절한 고지 또는 동의 없이 데이터를 유출하는 악성 코드 또는 동작도 스파이웨어로 간주됩니다.

예를 들어 스파이웨어 위반은 다음을 포함하되 이에 국한되지 않습니다.

- 음성 녹음 또는 전화에서 이루어지는 통화 녹음
- 앱 데이터 탈취
- 사용자가 예상하지 못한 방식 및/또는 적절한 사용자 고지 또는 동의 없이 데이터를 기기 밖으로 전송하는 악성 서드 파티 코드(예: SDK)가 포함된 앱

모든 앱은 원치 않는 모바일 소프트웨어, 사용자 데이터, 민감한 정보에 액세스하는 권한 및 API, SDK 요구사항과 같은 사용자 및 기기 데이터 정책을 비롯해 모든 Google Play 개발자 프로그램 정책도 준수해야 합니다.

트로이 목마

게임이라고만 주장하지만 사용자에게 바람직하지 않은 작업을 수행하는 게임과 같이 무해한 것처럼 보이는 코드입니다.

이 분류는 다른 PHA 카테고리와 함께 사용됩니다. 트로이 목마에는 무해한 구성요소와 숨겨진 유해 구성요소가 함께 있습니다. 사용자에게 알리지 않고 사용자 기기의 백그라운드에서 프리미엄 SMS 메시지를 보내는 게임을 예로 들 수 있습니다.

특수 앱 관련 참고사항

Google Play 프로텍트에서 앱이 안전하다고 판단할 만큼 정보가 충분하지 않은 경우 드물고 새로운 앱은 특수한 것으로 분류될 수 있습니다. 앱이 반드시 유해하다는 의미는 아니지만 추가적인 검토가 없다면 안전하다고 볼 수도 없습니다.

백도어 카테고리 관련 참고사항

백도어 멀웨어 카테고리 분류는 코드의 행동 방식을 따릅니다. 코드가 자동으로 실행될 경우 이 코드를 다른 멀웨어 카테고리 중 하나에 배치하는 동작을 설정하는 것이 코드가 백도어로 분류되기 위한 필수 조건입니다. 예를 들어, 앱에서 동적 코드 로딩을 허용하고 동적으로 로드된 코드가 SMS를 추출할 경우 백도어 멀웨어로 분류됩니다.

그러나 앱에서 임의의 코드 실행을 허용하며 Google에서 코드 실행이 악의적 행위를 목적으로 추가되었다고 판단할 만한 근거가 없다면 앱은 백도어 멀웨어가 아닌 취약점이 있는 앱으로 처리되며 개발자는 패치 요청을 받습니다.

마스크웨어

사용자에게 설명과 다르거나 가짜인 애플리케이션 기능을 제공하기 위해 다양한 회피 기법을 활용하는 애플리케이션입니다. 이러한 앱은 앱 스토어에서 무해하게 보이기 위해 적법한 애플리케이션 또는 게임인 것처럼 가장할 뿐만 아니라 난독화, 동적 코드 로딩 또는 클로킹과 같은 수법을 사용하여 악의적인 콘텐츠를 드러냅니다.

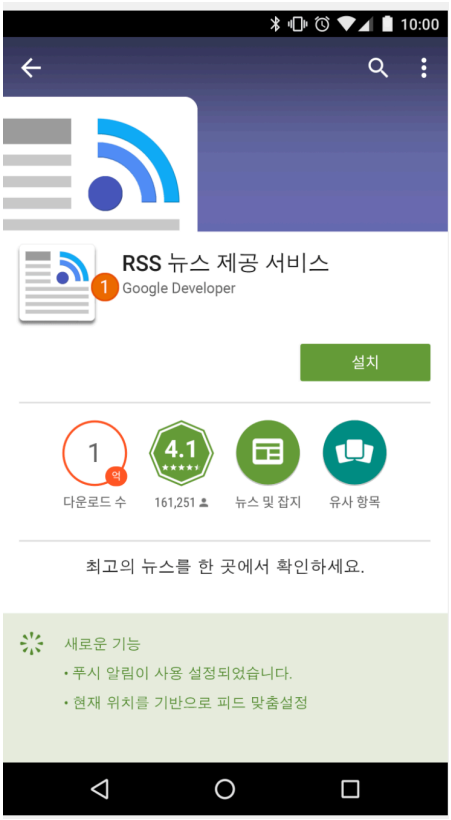
마스크웨어는 다른 PHA 카테고리, 특히 트로이 목마와 유사하며, 주요 차이점은 악의적인 활동을 난독화하는 데 사용하는 기법이 다르다는 점입니다.

명의 도용

다른 사람(예: 다른 개발자, 기업, 법인) 또는 다른 앱을 사칭하여 사용자를 오도하는 앱은 허용되지 않습니다. 앱이 실제와 다르게 다른 사람과 관계가 있거나 다른 사람의 승인을 받았다는 내용을 암시해서는 안 됩니다. 사용자가 앱과 다른 사람 또는 다른 앱의 관계를 오해할 만한 앱 아이콘, 설명, 제목 또는 인앱 요소를 사용하지 않도록 주의하세요.

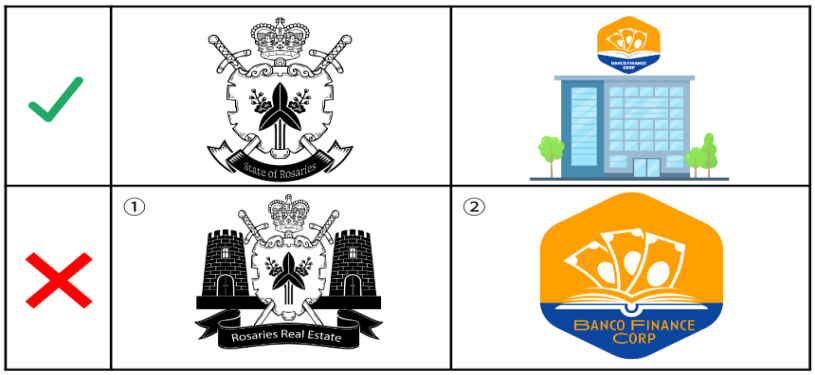
다음은 자주 발생하는 위반 사례입니다.

- 개발자가 다른 회사/개발자/단체/조직과의 관계를 허위로 암시합니다.



① 앱에 표시된 개발자 이름이 실제로는 관계가 없음에도 불구하고 마치 Google과 공식적인 관계가 있는 것 같은 인상을 줍니다.

- 앱 아이콘이나 제목이 다른 회사/개발자/단체/조직과의 관계를 허위로 암시합니다.



① 앱이 국가 상징물을 사용하여 정부와 관계가 있는 것처럼 사용자의 오해를 불러일으킵니다.
② 앱이 기업의 로고를 복사하여 해당 기업의 공식 앱인 것처럼 허위로 암시합니다.

- 앱 제목과 아이콘이 사용자가 오해할 정도로 기존 제품이나 서비스와 유사합니다.

① 앱 아이콘에 유명한 암호화폐 웹사이트 로고를 사용해 공식 웹사이트인 것처럼 암시합니다.
② 앱 아이콘에 유명한 TV 프로그램의 캐릭터와 제목을 그대로 사용하여 사용자가 TV 프로그램과 관련된 앱으로 생각하도록 오도합니다.

- 기존 법인의 공식 앱인 것처럼 허위로 주장하는 앱입니다. 필요한 허가 또는 권리 없이는 '저스틴 비버 공식 앱'과 같은 제목을 사용할 수 없습니다.

- Android 브랜드 가이드라인 을 위반하는 앱입니다.

원치 않는 모바일 소프트웨어

Google은 사용자에게 초점을 맞추면 나머지는 저절로 따라온다고 믿습니다. 소프트웨어 정책과 원치 않는 소프트웨어 정책에서 Google은 우수한 사용자 환경을 구현하는 소프트웨어에 관한 일반적인 권장사항을 제공합니다. Android 생태계와 Google Play 스토어의 원칙에 관해 간략히 설명하는 이 정책은 Google의 '원치 않는 소프트웨어 정책'을 기반으로 합니다. 아래에 나열된 원칙을 위반하는 소프트웨어는 사용자 환경에 잠재적으로 해롭기 때문에 Google은 이러한 소프트웨어로부터 사용자를 보호하기 위한 조치를 취합니다.

'원치 않는 소프트웨어 정책'에 명시된 바와 같이 대부분의 원치 않는 소프트웨어에는 다음과 같이 공통적인 기본 특징이 하나 이상 있다는 사실을 발견했습니다.

- 실제로는 제공하지 않는 가치 제안을 약속하여 사용자를 속입니다.
- 사용자를 속여서 설치하게 하거나 다른 프로그램을 설치할 때 몰래 설치되기도 합니다.
- 사용자에게 주요 기능을 모두 알리지 않습니다.
- 예상치 못한 방식으로 사용자의 시스템에 영향을 미칩니다.
- 사용자 모르게 개인 정보를 수집하거나 전송합니다.
- 보안 조치(예: HTTPS를 통한 전송) 없이 개인 정보를 수집하거나 전송합니다.
- 다른 소프트웨어와 번들로 제공되며 존재가 공개되지 않습니다.

휴대기기에서 소프트웨어란 앱, 바이너리, 프레임워크 수정과 같은 형태의 코드입니다. 소프트웨어가 소프트웨어 생태계에 유해한 영향을 미치거나 사용자 경험을 저해하지 않도록 하기 위해 Google은 이러한 원칙을 위반하는 코드를 대상으로 조치를 취하고 있습니다.

모바일 소프트웨어로 적용 대상을 확장하기 위해 아래와 같이 '원치 않는 소프트웨어 정책]을 마련해 두었습니다. 이 정책과 더불어 Google은 새로운 유형의 악용 사례에 대응할 수 있도록 이 원치 않는 모바일 소프트웨어 정책을 지속적으로 개선할 예정입니다.

투명한 행동과 명확한 공개

모든 코드는 사용자에게 약속한 내용을 전달해야 합니다. 앱은 안내한 모든 기능을 제공해야 합니다. 앱은 사용자의 혼란을 유도하지 않아야 합니다.

- 앱은 그 기능과 목적이 명확해야 합니다.
- 앱으로 인해 어떤 시스템 변경사항이 있는지를 사용자에게 명시적이고 분명하게 설명합니다. 사용자가 주요한 설치 옵션과 변경사항을 모두 검토하고 승인하도록 허용합니다.
- 소프트웨어는 사용자에게 사용자 기기의 상태를 허위로 표시해서는 안 됩니다. 시스템이 보안상 심각한 상태 또는 바이러스에 감염된 상태라고 주장하는 경우를 예로 들 수 있습니다.
- 광고 트래픽 및/또는 전환을 높이기 위한 무효 활동을 활용해서는 안 됩니다.
- 다른 사람(예: 다른 개발자, 기업, 법인) 또는 다른 앱을 사칭하여 사용자의 오해를 불러일으키는 앱은 허용되지 않습니다. 앱이 실제와 다르게 다른 사람과 관계가 있거나 다른 사람의 승인을 받았다는 내용을 암시해서는 안 됩니다.

위반 예시:

- 광고 사기
- 소셜 엔지니어링

사용자 데이터 및 개인 정보 보호

개인 정보 및 민감한 사용자 데이터의 액세스, 사용, 수집, 공유에 관해 명확하고 투명하게 공개합니다. 사용자 데이터 사용 시에는 적용되는 모든 관련 사용자 데이터 정책을 준수하고 데이터 보호를 위한 모든 예방 조치를 취해야 합니다.

모든 앱은 사용자 데이터, 민감한 정보에 액세스하는 권한 및 API, 스파이웨어, SDK 요구사항과 같은 사용자 및 기기 데이터 정책을 비롯해 모든 Google Play 개발자 프로그램 정책을 준수해야 합니다.

- 사용자가 Google Play 프로텍트와 같은 기기 보안 보호 기능을 사용 중지하도록 요청하거나 오도해서는 안 됩니다. 예컨대 Google Play 프로텍트를 사용 중지하는 대가로 사용자에게 추가 앱 기능 또는 리워드를 제공해서는 안 됩니다.

모바일 환경 저해하지 않기

사용자 환경은 직관적이고 이해하기 쉬우며 사용자의 분명한 선택에 기반을 두어야 합니다. 사용자에게 명확하게 가치를 제안해야 하며, 광고된 사용자 환경 또는 바람직한 사용자 환경을 방해해서는 안 됩니다.

- 기기 기능의 사용성을 저해하거나 방해하는 방식 또는 적절한 동의와 저작자 표시 없이 실행 중인 앱 환경 외부에 표시되어 쉽게 취소할 수 없는 방식과 같이 예상치 못한 방식으로 사용자에게 광고를 표시해서는 안 됩니다.
- 앱이 다른 앱 또는 기기의 사용성을 방해하지 않아야 합니다.

- 해당하는 경우 제거 방법이 명확해야 합니다.
- 모바일 소프트웨어는 기기 OS 또는 다른 앱의 메시지를 모방해서는 안 됩니다. 다른 앱 또는 운영체제의 알림, 특히 사용자에게 OS의 변경사항을 알리는 알림을 숨겨서는 안 됩니다.

위반 예시:

- 불편을 야기하는 광고
- 시스템 기능 무단 사용 또는 모방

적대적인 다운로더

그 자체로 원치 않는 소프트웨어는 아니지만 다른 원치 않는 모바일 소프트웨어(MUwS: Mobile Unwanted Software)를 다운로드하는 코드입니다.

다음 중 하나에 해당할 경우 코드가 적대적인 다운로더일 수 있습니다.

- MUwS를 퍼뜨리기 위해 만들어졌다고 믿을 만한 근거가 있으며, MUwS를 다운로드했거나 앱을 다운로드하고 설치할 수 있는 코드가 포함된 경우
- 확인된 앱 다운로드 최소 기준값 500건 중 다운로드된 앱 5% 이상이 MUwS인 경우(25건의 확인된 MUwS 다운로드)

주요 브라우저와 파일 공유 앱은 다음에 모두 해당할 경우 적대적 다운로더로 간주하지 않습니다.

- 사용자 상호작용 없이 다운로드를 유도하지 않는 경우
- 모든 소프트웨어 다운로드가 사용자의 동의에 따라 시작되는 경우

광고 사기

광고 사기는 엄격히 금지됩니다. 트래픽이 실제 사용자 관심에서 비롯된 것으로 믿도록 광고 네트워크를 속이기 위해 생성된 광고 상호작용을 광고 사기라고 하며, 이는 무효 트래픽의 한 형태입니다. 광고 사기는 개발자가 숨겨진 광고 표시, 광고 자동 클릭, 정보 변경 또는 수정, 스파이더, 봇 등의 비인간 작업이나 무효 광고 트래픽 생산을 위한 인간 활동의 활용과 같이 허용되지 않는 방식으로 광고를 구현한 결과로 발생할 수 있습니다. 무효 트래픽 및 광고 사기는 광고주, 개발자, 사용자에게 유해하며 이로 인해 모바일 광고 생태계가 장기적인 신뢰를 잃게 됩니다.

다음은 자주 발생하는 위반 사례입니다.

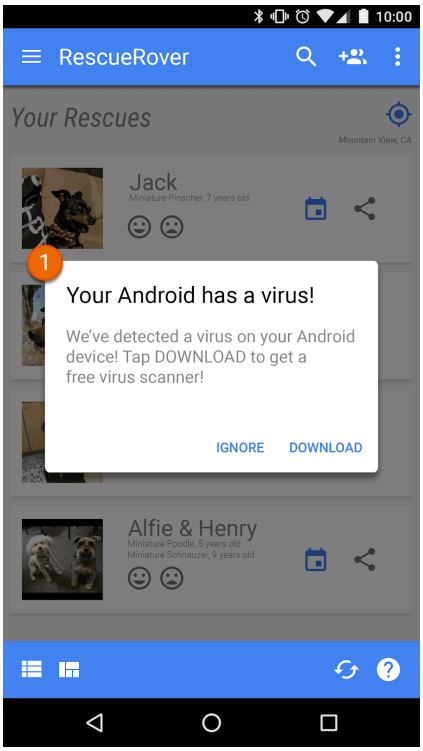
- 사용자에게 보이지 않는 광고를 렌더링하는 앱
- 사용자가 의도하지 않게 광고를 자동으로 클릭하게 하거나 상응하는 네트워크 트래픽을 생성하여 부정한 방식으로 클릭수 크레딧을 부여하는 앱
- 전송자의 네트워크에서 발생하지 않은 설치로 보상을 받기 위해 가짜 설치 기여 분석 클릭수를 전송하는 앱
- 사용자가 앱 인터페이스 내에 있지 않을 때 광고를 표시하는 앱
- 실제로는 Android 기기에서 실행 중인데 iOS 기기에서 실행 중이라고 광고 네트워크에 알리는 앱, 수익 창출에 사용 중인 패키지 이름을 허위로 표시하는 앱과 같이 광고 인벤토리를 허위로 기재하는 앱

시스템 기능 무단 사용 또는 모방

앱 또는 광고가 알림, 경고 등과 같은 시스템 기능을 모방하거나 방해해서는 안 됩니다. 시스템 수준 알림은 특가 요금을 알리는 항공사 앱 또는 인게임 프로모션을 알리는 게임과 같이 앱의 필수적인 기능에만 사용해야 합니다.

다음은 자주 발생하는 위반 사례입니다.

- 시스템 알림 또는 경고를 통해 게재된 앱 또는 광고입니다.



① 이 앱에 표시된 시스템 알림은 광고를 게재하기 위해 사용됩니다.

광고와 관련된 추가 예는 광고 정책을 참고하세요.

소셜 엔지니어링

사용자가 원래 신뢰하는 앱에서 진행하려고 한 작업을 하도록 속이기 위해 다른 앱인 것처럼 가장하는 앱은 허용되지 않습니다.

수익 창출 및 광고

Google Play는 유료 배포, 인앱 상품, 정기 결제, 광고 기반 모델과 같이 개발자와 사용자에게 혜택을 제공할 수 있는 다양한 수익 창출 전략을 지원합니다. 최고의 사용자 환경을 구현하려면 본 정책을 준수해야 합니다.

결제

1. Google Play에서 이루어지는 앱 다운로드에 요금을 청구하려는 개발자는 해당 거래의 결제 수단으로 Google Play 결제 시스템을 사용해야 합니다.
2. Play에서 배포되는 앱은 앱 기능, 디지털 콘텐츠 또는 상품을 포함한 인앱 기능 또는 서비스 이용을 위한 결제를 요구하거나 수락하는 경우('인앱 구매'로 통칭) 3항, 8항 또는 9항이 적용되지 않는 한, 해당 거래의 결제에 Google Play의 결제 시스템을 사용해야 합니다.

    Google Play의 결제 시스템을 사용해야 하는 앱 기능 또는 서비스의 예로는 다음의 인앱 구매가 포함되지만 이에 국한되지 않습니다.

    - 아이템(예: 가상 화폐, 추가 생명력, 추가 플레이 시간, 부가기능 아이템, 캐릭터, 아바타)
    - 정기 결제 서비스(예: 피트니스, 게임, 데이트, 교육, 음악, 동영상, 서비스 업그레이드, 기타 콘텐츠 정기 결제 서비스)
    - 앱 기능 또는 콘텐츠(예: 광고 없는 버전의 앱 또는 무료 버전에서는 사용할 수 없는 새로운 기능 등)

- 클라우드 소프트웨어 및 서비스(예: 데이터 스토리지 서비스, 비즈니스 생산성 소프트웨어, 재무 관리 소프트웨어)

3. 다음의 경우에는 Google Play 결제 시스템을 사용해서는 안 됩니다.
   a. 결제가 주로 다음과 같은 구매에서 이루어지는 경우:
      - 실제 상품(예: 식료품, 의류, 가정용품, 전자제품)의 구매 또는 대여
      - 실제 서비스(예: 교통 서비스, 청소 서비스, 항공 운임, 헬스클럽 회원권, 음식 배달, 실시간 이벤트 티켓)의 구매
      - 신용카드 고지서 또는 공과금 고지서(예: 케이블 및 통신 서비스) 관련 송금
   b. P2P 결제, 온라인 경매, 세금 면제 기부가 포함되어 있는 결제
   c. 실제 현금 도박, 게임, 콘텐츠 정책의 도박 앱 섹션에 설명되어 있는 바와 같이 온라인 도박을 조장하는 콘텐츠 또는 서비스의 결제
   d. Google의 결제 센터 콘텐츠 정책 에 따라 허용되지 않는 것으로 간주되는 제품 카테고리와 관련된 결제

      참고: 일부 시장에서는 실제 상품 및/또는 서비스를 판매하는 앱을 대상으로 Google Pay를 제공합니다. 자세한 내용은 Google Pay 개발자 페이지를 참고하세요.

4. 3항, 8항, 9항에 명시된 조건 이외에는 Google Play 결제 시스템 이외의 결제 수단으로 사용자를 유도할 수 없습니다. 이러한 금지 대상에는 다음을 통해 사용자를 다른 결제 수단으로 유도하는 행위가 포함되나 이에 국한되지 않습니다.
   - Google Play의 앱 등록정보
   - 구매 가능한 콘텐츠와 관련된 인앱 프로모션
   - 인앱 WebView, 버튼, 링크, 메시지, 광고 또는 기타 클릭 유도 문구
   - 앱 사용자를 Google Play 결제 시스템이 아닌 결제 수단으로 유도하는 계정 생성 또는 가입 절차 등의 인앱 사용자 인터페이스 흐름
5. 인앱 가상 통화는 구매한 앱 또는 게임 내에서만 사용되어야 합니다.
6. 개발자는 판매하는 앱 또는 인앱 기능이나 정기 결제의 조건 및 가격과 관련하여 사용자에게 명확하고 정확한 정보를 제공해야 합니다. 인앱 가격은 사용자에게 표시되는 Play 결제 인터페이스에 표시되는 가격과 일치해야 합니다. Google Play의 제품 설명에 특정 비용 또는 추가 비용이 요구될 수 있는 인앱 기능이 언급된 경우, 이러한 기능을 이용하려면 결제가 필요하다는 점을 앱 등록정보를 통해 사용자에게 명확히 알려야 합니다.
7. 구매를 통해 무작위 가상 상품을 받는 메커니즘('전리품 상자'를 포함하되 이에 국한되지 않음)을 제공하는 앱과 게임은 구매가 이루어지기 전, 그리고 구매 시점과 근접한 시간에 관련 아이템을 받을 확률을 명확하게 공개해야 합니다.
8. 3항에 명시된 조건에 해당되지 않는 한 Play 배포 앱의 개발자가 인앱 구매 이용을 위해 이러한 국가/지역의 사용자에게 결제를 요구하거나 사용자의 결제를 수락하는 경우, 각 관련 프로그램의 결제 선언 양식을 작성하고 해당 양식에 포함된 추가 약관 및 프로그램 요구사항에 동의하면 해당 거래에 Google Play의 결제 시스템과 함께 개발자 제공 결제 시스템을 사용자에게 제공할 수 있습니다.
9. Play 배포 앱의 개발자는 디지털 인앱 기능 및 서비스 혜택 홍보 등의 목적으로 유럽 경제 지역(EEA) 사용자를 앱 외부로 안내할 수 있습니다. EEA 사용자를 앱 외부로 안내하는 개발자는 프로그램의 선언 양식을 작성하고 해당 양식에 포함된 추가 약관 및 프로그램 요구사항에 동의해야 합니다.

참고: 이 정책에 관한 타임라인과 자주 묻는 질문(FAQ)을 보려면 고객센터를 방문하세요.

광고

우수한 경험을 유지하기 위해 Google에서는 광고의 콘텐츠, 잠재고객, 사용자 경험, 행동, 보안 및 개인 정보 보호를 고려합니다. 광고 및 관련 혜택은 앱의 일부분으로 간주되며, 기타 모든 Google Play 정책을 준수해야 합니다. 또한 Google Play에서 아동을 대상으로 하는 앱으로 수익을 창출하는 경우 추가 광고 요건이 적용됩니다.

여기에서 Google이 사용자를 기만하는 프로모션 관행을 처리하는 방법을 비롯해 앱 프로모션 및 스토어 등록정보 정책에 대해 자세히 알아볼 수 있습니다.

광고 콘텐츠

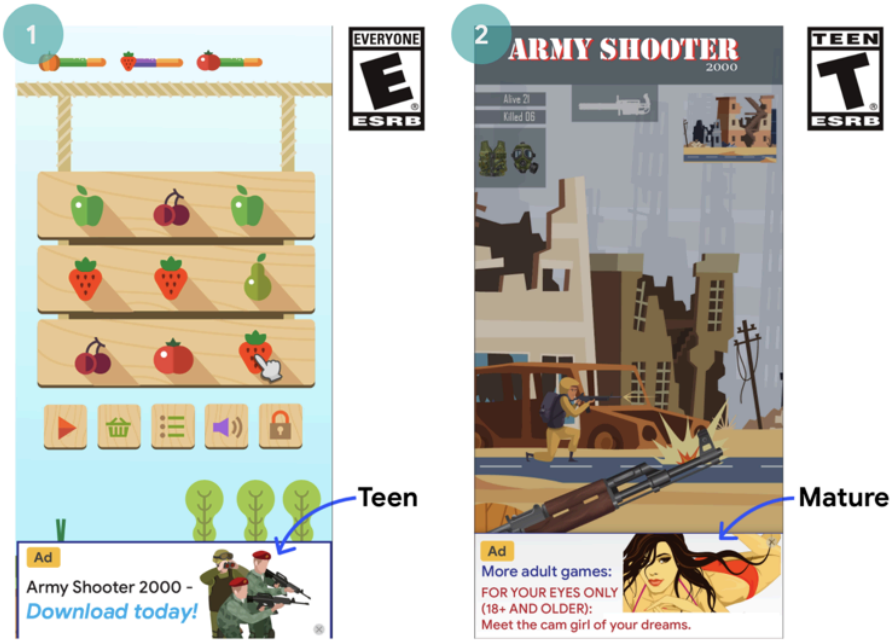
광고 및 관련 혜택은 앱의 일부분이며 Google의 제한된 콘텐츠 정책을 준수해야 합니다. 앱이 도박 앱인 경우 추가 요건이 적용됩니다.

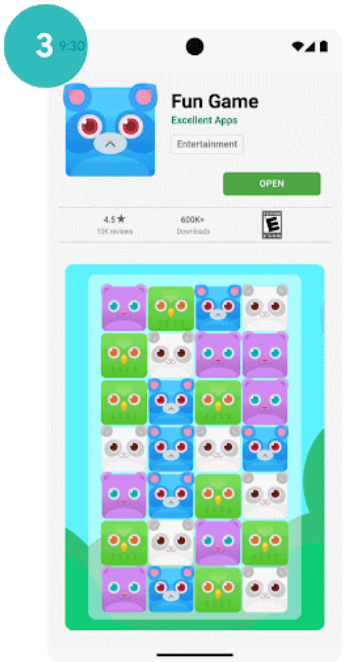
부적절한 광고

앱 내에 표시되는 광고 및 관련 혜택(예: 다른 앱의 다운로드를 홍보하는 광고)은 콘텐츠 자체가 Google 정책을 준수하더라도 앱의 콘텐츠 등급 에 적합해야 합니다.

다음은 자주 발생하는 위반 사례입니다.

- 앱의 콘텐츠 등급에 부적절한 광고입니다.





① 이 광고는 앱의 콘텐츠 등급(전체이용가)에 부적절합니다(청소년).
② 이 광고는 앱의 콘텐츠 등급(청소년)에 부적절합니다(성인).
③ 광고의 혜택(성인용 앱 다운로드 프로모션)이 광고가 표시된 게임 앱의 콘텐츠 등급(전체이용가)에 부적절합니다.

가족 광고 요건

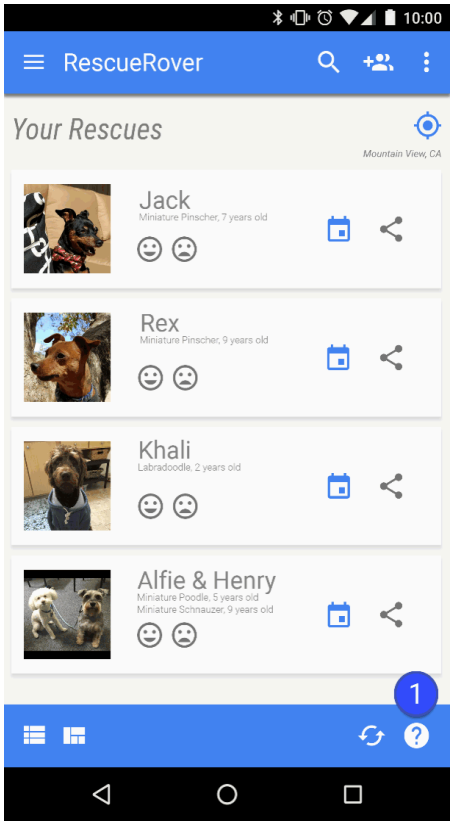
Google Play에서 아동을 대상으로 하는 앱으로 수익을 창출하는 경우 앱은 가족 광고 및 수익 창출 정책 요건을 준수해야 합니다.

사기성 광고

광고는 운영체제의 알림 또는 경고와 같이 앱 기능을 위한 사용자 인터페이스인 것처럼 가장하거나 속여서는 안 됩니다. 각 광고가 어떤 앱에서 게재되었는지 사용자가 명확히 알 수 있어야 합니다.

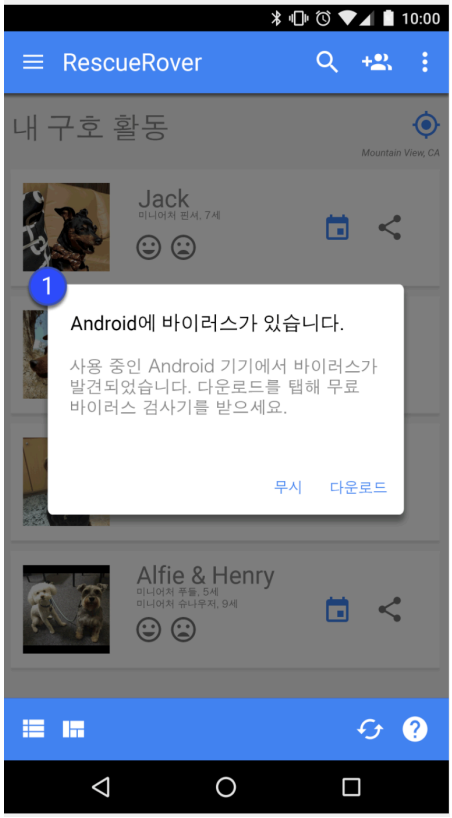
다음은 자주 발생하는 위반 사례입니다.

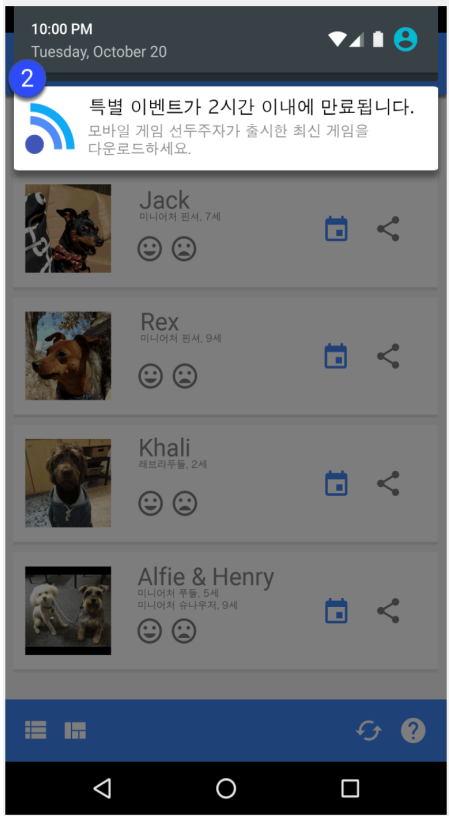
- 앱의 UI를 모방한 광고입니다.



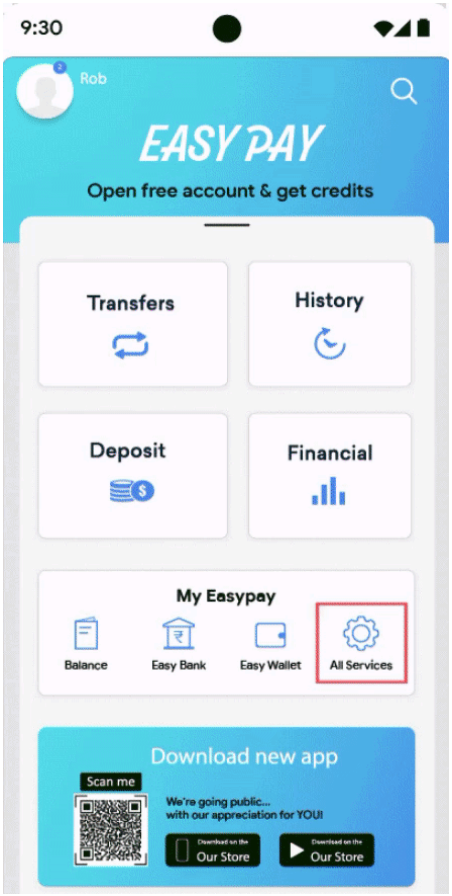
① 이 앱에 있는 물음표 아이콘은 사용자를 외부 방문 페이지로 리디렉션하는 광고입니다.

- 시스템 알림을 모방한 광고입니다.





① ② 위의 예는 다양한 시스템 알림을 모방한 광고를 보여줍니다.



① 위의 기능 섹션은 다른 기능을 모방하고 있지만 실제로는 사용자를 광고로 연결하는 역할만 합니다.

불편을 야기하는 광고

불편을 야기하는 광고란 예상치 못한 방식으로 표시되어 의도치 않은 클릭 또는 기기 기능의 사용성 저해나 방해로 이어질 수 있는 광고를 말합니다.

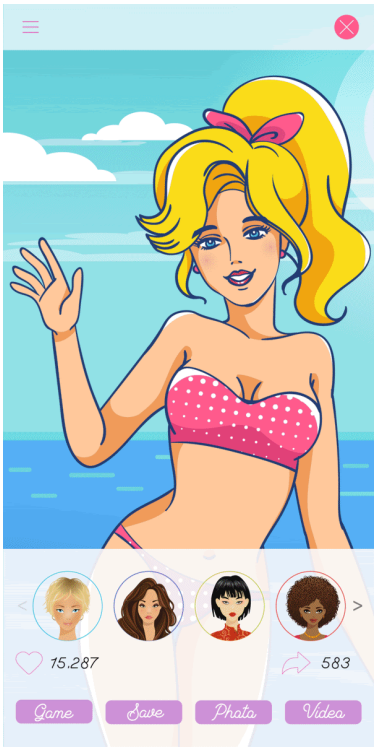
앱은 사용자가 앱을 완전히 사용할 수 있게 되기 전에 광고를 클릭하게 하거나 광고 목적으로 개인 정보를 제출하게 할 수 없습니다. 광고는 광고가 게재되는 앱의 내부에만 표시될 수 있으며, 시스템/기기 버튼 및 포트를 비롯해 다른 앱, 광고 또는 기기의 작동을 방해해서는 안 됩니다. 여기에는 오버레이, 컴패니언 기능, 위젯화된 광고 단위가 포함됩니다. 앱에서 정상적인 사용을 방해하는 광고 또는 기타 광고를 표시하는 경우 불이익 없이 간편하게 닫을 수 있어야 합니다.

다음은 자주 발생하는 위반 사례입니다.

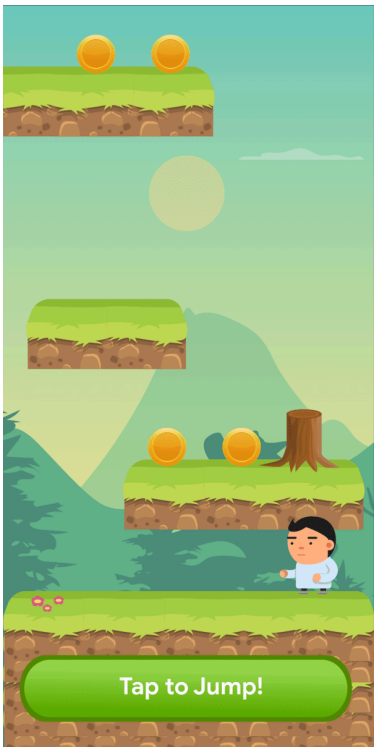
- 전체 화면을 차지하거나 정상적인 사용을 방해하며 광고를 닫는 명확한 방법이 마련되어 있지 않은 광고입니다.

① 이 광고에는 닫기 버튼이 없습니다.

- 가짜 닫기 버튼을 사용하거나 다른 기능을 위해 사용자가 자주 탭하는 앱 영역에 갑자기 광고를 표시하여 클릭하도록 하는 광고입니다.

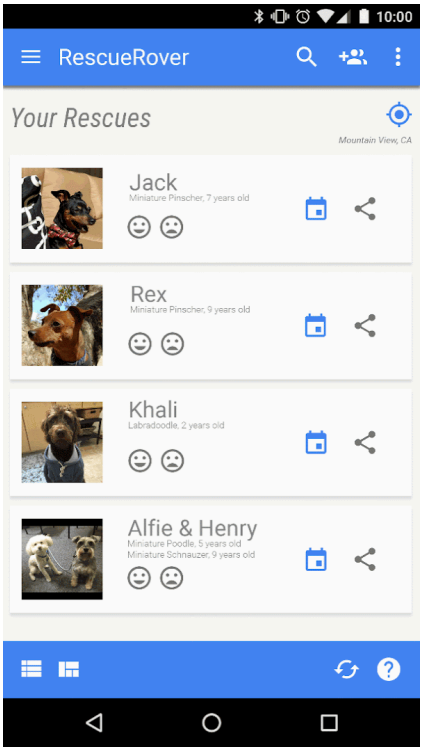


① 이 광고에서는 가짜 닫기 버튼을 사용합니다.



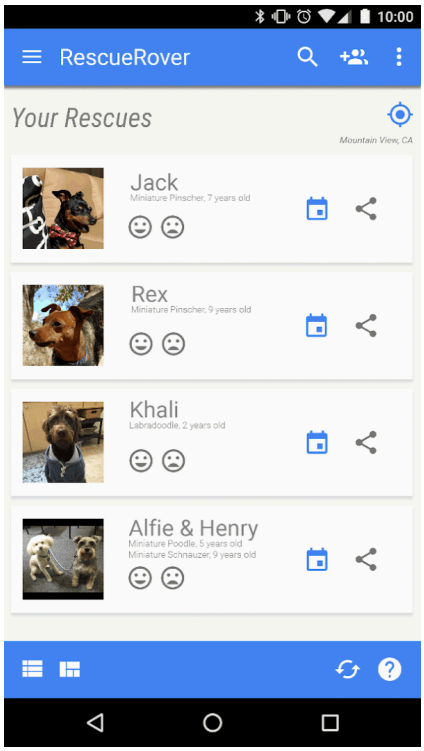
② 사용자가 인앱 기능을 사용하기 위해 탭하는 영역에 이 광고가 갑자기 나타납니다.

- 광고가 게재되는 앱의 외부에 표시되는 광고입니다.



① 사용자가 앱에서 홈 화면으로 이동하는데 갑자기 홈 화면에 광고가 표시됩니다.

- 홈 버튼 또는 앱을 종료하도록 명시적으로 설계된 기타 기능에 의해 실행되는 광고입니다.



① 사용자가 앱을 종료하고 홈 화면으로 이동하려는데 광고가 정상적인 흐름을 끊고 예기치 않게 표시됩니다.

더 나은 광고 경험(Better Ads Experiences)

개발자는 사용자가 Google Play 앱을 사용할 때 양질의 경험을 누릴 수 있도록 다음 광고 가이드라인을 준수해야 합니다. 다음과 같이 예상치 못한 방식으로 사용자에게 광고를 표시할 수 없습니다.

- 일반적으로 사용자가 다른 동작을 하기로 선택했을 때 예상치 못하게 나타나는 모든 형식의 전체 화면 전면 광고(동영상, GIF, 정적 광고 등)는 허용되지 않습니다.
  - 게임 플레이 도중에 레벨 시작 시 또는 콘텐츠 세그먼트 시작 중에 나타나는 광고는 허용되지 않습니다.
  - 앱 로딩 화면(스플래시 화면) 전에 나타나는 전체 화면 동영상 전면 광고는 허용되지 않습니다.
- 15초가 지난 후에도 닫을 수 없는 모든 형식의 전체 화면 전면 광고는 허용되지 않습니다. 선택형 전체 화면 전면 광고 또는 사용자의 작업을 방해하지 않는(예: 게임 앱의 점수 화면 이후에 표시) 전체 화면 전면 광고는 15초 넘게 지속될 수 있습니다.

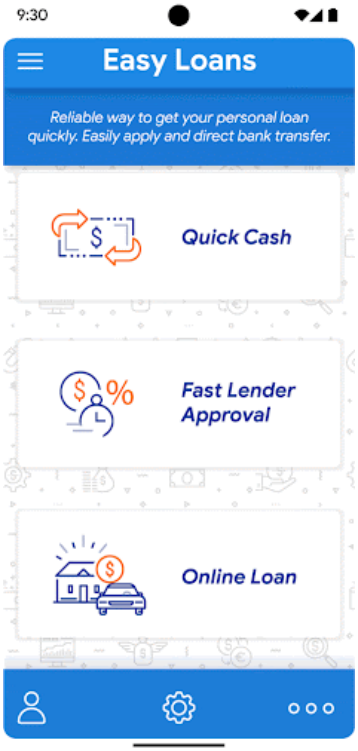
사용자가 명시적으로 선택한 보상형 광고에는 이 정책이 적용되지 않습니다(예: 개발자가 특정 게임 기능 또는 콘텐츠의 잠금 해제를 대가로 사용자에게 명시적으로 시청을 제안하는 광고). 이 정책은 정상적인 앱 사용 또는 게임 플레이를 방해하지 않는 수익 창출 및 광고에도 적용되지 않습니다(예: 광고가 통합된 동영상 콘텐츠, 전체 화면이 아닌 배너 광고).

이 가이드라인은 더 나은 광고 표준(Better Ads Standard) - 모바일 앱 환경 가이드라인을 참고하였습니다. 더 나은 광고 표준(Better Ads Standard)에 관한 자세한 내용은 더 나은 광고 연합(Coalition for Better Ads) 을 참고하세요.

다음은 자주 발생하는 위반 사례입니다.

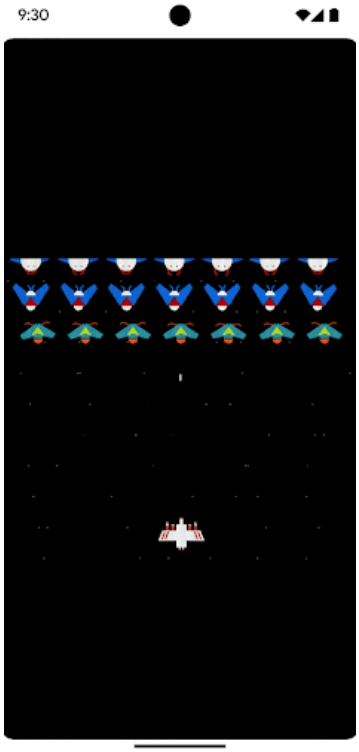
- 게임 플레이 도중에 또는 콘텐츠 세그먼트 시작 중에 나타나는 예상치 못한 광고(예: 사용자가 버튼을 클릭한 후 버튼 클릭으로 의도한 동작이 실행되기 전). 사용자는 게임이 시작되거나 콘텐츠가 표시될 것이라고 예상하므로 이러한 광고는 사용자가 예상치 못한 것입니다.

① 예상치 못한 정적 광고가 게임 플레이 도중에 레벨 시작 시 나타납니다.



② 예상치 못한 동영상 광고가 콘텐츠 세그먼트 시작 중에 나타납니다.

- 게임 플레이 도중에 나타나고 15초가 지난 후에도 닫을 수 없는 전체 화면 광고



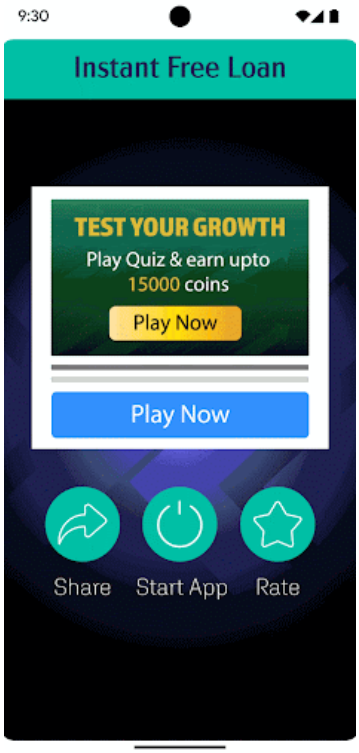
① 전면 광고가 게임 플레이 도중에 나타나고 15초 이내에 사용자에게 건너뛸 수 있는 옵션을 제공하지 않습니다.

광고 게시용 앱

전면 광고를 반복적으로 표시해 사용자가 앱과 상호작용하거나 앱 내 작업을 수행하지 못하게 방해하는 앱은 허용되지 않습니다.

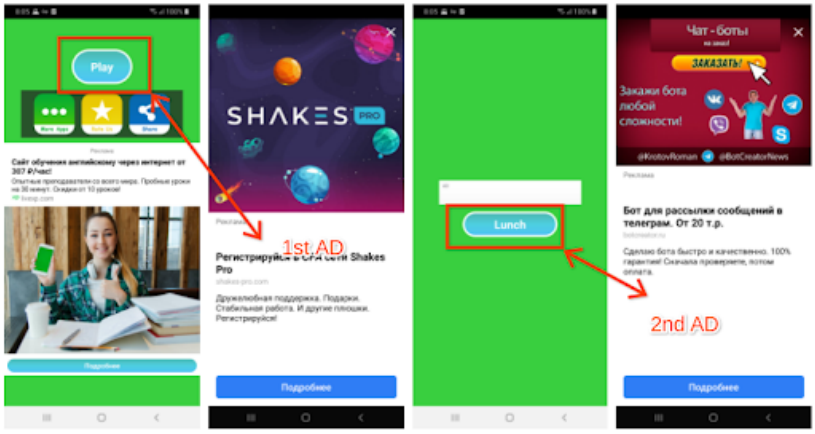
다음은 자주 발생하는 위반 사례입니다.

- 사용자 작업(클릭, 스와이프를 포함하되 이에 국한되지 않음) 이후 연속적으로 전면 광고가 표시되는 앱



① 첫 번째 인앱 페이지에는 상호작용할 수 있는 버튼이 여러 개 있습니다. 사용자가 앱을 사용하기 위해 **Start app**(앱 시작)을 클릭하면 전면 광고가 뜹니다. 광고를 닫고 나서 사용자가 앱으로 돌아가 서비스를 사용하기 위

해 **Service**(서비스)를 클릭하면 또 다른 전면 광고가 나타납니다.



② 첫 번째 페이지에는 **Play**(플레이) 버튼만 표시되므로 사용자는 앱을 사용하기 위해 이를 클릭하게 됩니다. 이 버튼을 클릭하면 전면 광고가 나타납니다. 광고를 닫은 후 사용자가 상호작용할 수 있는 유일한 버튼인 **Launch**(시작)를 클릭하면 또 다른 전면 광고가 뜹니다.

잠금 화면을 통한 수익 창출

앱의 유일한 목적이 잠금 화면을 통한 수익 창출이 아닌 이상, 기기의 잠금 화면을 통해 수익을 창출하는 광고나 기능을 앱에 추가할 수 없습니다.

광고 사기

광고 사기는 엄격히 금지됩니다. 자세한 내용은 Google의 광고 사기 정책을 참고하세요.

광고를 위한 위치 데이터 사용

광고 게재를 위해 권한 기반 기기 위치 데이터의 사용을 확장하는 앱에는 개인 정보와 민감한 정보 정책이 적용되며 이러한 앱은 다음 요구사항을 반드시 준수해야 합니다.

- 광고 목적으로 권한 기반 기기 위치 데이터를 사용 또는 수집할 경우, 위치 데이터 사용을 다루는 관련 광고 네트워크 개인정보처리방침을 링크하는 방식 등으로 이 사실을 사용자에게 명확하게 설명하고 앱의 필수 개인정보처리방침에 문서화해야 합니다.
- 위치 정보 액세스 권한 요구사항에 따라 위치 정보 액세스 권한은 앱 내의 현재 기능 또는 서비스를 구현하기 위해서만 요청할 수 있으며, 광고 사용 목적만으로는 기기 위치 정보 액세스 권한을 요청할 수 없습니다.

Android 광고 ID 사용

Google Play 서비스 버전 4.0에서는 광고 및 분석 제공업체에서 사용할 수 있는 새 API 및 ID를 도입했습니다. 이러한 ID 사용에 관한 약관은 아래와 같습니다.

- **용도**: Android 광고 식별자(AAID)는 광고 및 사용자 분석에만 사용해야 합니다. 각 ID 액세스에서 '관심 기반 광고 선택 해제' 또는 '광고 개인 최적화 선택 해제' 설정 상태를 확인해야 합니다.
- **개인 식별 정보 또는 기타 식별자와 연결**
  - 광고 목적: 광고 ID는 광고 목적으로 영구적인 기기 식별자(예: SSAID, MAC 주소, IMEI 등)에 연결될 수 없습니다. 광고 ID는 사용자의 명시적 동의가 있어야 개인 식별 정보에 연결될 수 있습니다.
  - 분석 목적: 광고 ID는 분석 목적으로 개인 식별 정보 또는 영구적인 기기 식별자(예: SSAID, MAC 주소, IMEI 등)에 연결될 수 없습니다. 영구적인 기기 식별자에 관한 추가 가이드라인은 사용자 데이터 정책 에서 확인하세요.
- **사용자의 선택 존중**
  - 재설정 시 사용자의 명시적인 동의 없이 새 광고 ID를 기존 광고 ID 또는 기존 광고 ID에서 파생된 데이터에 연결하면 안 됩니다.
  - 사용자의 '관심 기반 광고 선택 해제' 또는 '광고 개인 최적화 선택 해제' 설정을 준수해야 합니다. 사용자가 이 설정을 사용하는 경우 광고 ID를 사용하여 광고 목적으로 사용자 프로필을 만들거나 개인 맞춤 광고로 사용자

를 타겟팅하면 안 됩니다. 허용되는 작업으로는 문맥 광고, 최대 게재빈도 설정, 전환 추적, 보고 및 보안, 사기 감지 등이 있습니다.
  - 새로운 기기에서 사용자가 Android 광고 ID를 삭제하면 ID는 삭제됩니다. 삭제된 ID에 액세스하려고 시도하면 0으로 된 문자열이 반환됩니다. 광고 ID가 없는 기기는 기존의 광고 ID에 연결되어 있거나 이로부터 파생된 데이터에 연결되어서는 안 됩니다.
- **사용자에게 투명하게 정보 공개**: 광고 ID의 수집과 사용 및 관련 약관을 준수하기 위한 노력은 법적으로 적합한 개인 정보 보호 고지를 통해 사용자에게 공개되어야 합니다. 개인 정보 보호 표준을 자세히 알아보려면 사용자 데이터 정책을 검토하세요.
- **이용약관 준수**: 광고 ID는 'Google Play 개발자 프로그램 정책'에 따라서만 사용할 수 있으며, 비즈니스 진행 과정에서 광고 ID를 공유할 수 있는 모든 당사자의 경우에도 마찬가지입니다. Google Play에 업로드되거나 게시되는 모든 앱은 광고 목적으로 다른 기기 식별자 대신 광고 ID(기기에서 사용 가능한 경우)를 사용해야 합니다.

자세한 내용은 Google의 사용자 데이터 정책을 참고하세요.

정기 결제

개발자는 앱 내에서 제공하는 정기 결제 서비스나 콘텐츠에 관해 사용자를 오도해서는 안 됩니다. 모든 인앱 프로모션 또는 스플래시 화면에서 명확한 정보를 전달하는 것이 중요합니다. 사용자에게 사기성 또는 조작된 구매 경험을 제공하는 앱(인앱 구매 또는 정기 결제 포함)은 허용되지 않습니다.

혜택에 관해 투명하게 설명해야 합니다. 여기에는 혜택의 조건, 정기 결제 가격, 결제 주기 빈도, 앱을 사용하려면 정기 결제가 필요한지 등을 명확하게 설명하는 것이 포함됩니다. 사용자는 추가적인 조치를 취하지 않고도 이러한 정보를 검토할 수 있어야 합니다.

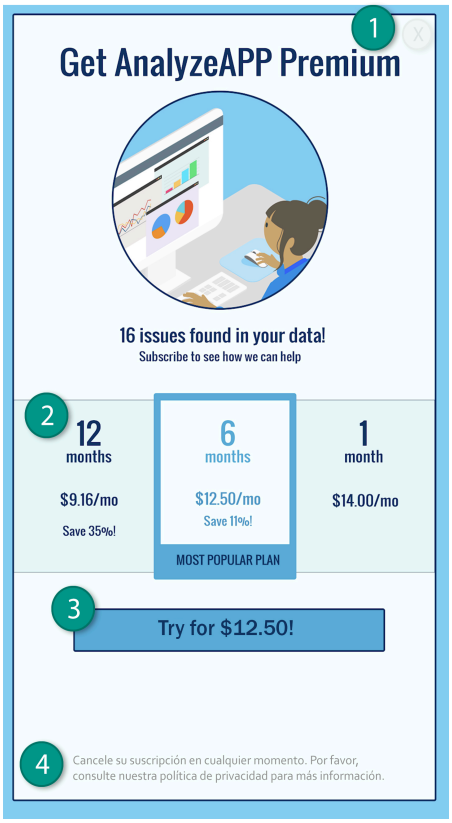
정기 결제는 계약 기간이 끝날 때까지 사용자에게 지속적이거나 반복적인 가치를 제공해야 하며 사용자에게 사실상의 일회성 혜택(예: 일시불 인앱 크레딧/통화 또는 일회용 게임 부스터를 제공하는 SKU)을 제공하는 데 사용될 수 없습니다. 정기 결제를 통해 인센티브나 프로모션 보너스를 제공할 수는 있지만 이는 정기 결제 기간 중 제공되는 지속적이거나 반복적인 가치를 보완하는 개념이어야 합니다. 지속적이고 반복적인 가치를 제공하지 않는 제품은 정기 결제 제품 대신 인앱 상품을 사용해야 합니다.

사용자에게 제공되는 일회성 혜택을 정기 결제로 위장하거나 잘못 설명해서는 안 됩니다. 여기에는 사용자가 정기 결제를 신청한 후에 정기 결제를 수정하여 일회성 혜택으로 바꾸는 행위(예: 반복적으로 제공되는 가치의 취소, 지원 중단 또는 최소화)가 포함됩니다.

다음은 자주 발생하는 위반 사례입니다.

- 월별 정기 결제에서 사용자에게 정기 결제가 자동 갱신되어 매달 요금이 청구된다는 사실을 알리지 않습니다.
- 연간 정기 결제에서 월간 정기 결제 가격을 가장 두드러지게 표시합니다.
- 정기 결제 가격 및 약관이 완전히 현지화되어 있지 않습니다.
- 인앱 프로모션에서 정기 결제 없이도 콘텐츠에 액세스할 수 있다는 점(가능한 경우)을 명확하게 설명하지 않습니다.
- SKU 이름이 정기 결제의 성격을 정확하게 전달하지 않습니다. 예를 들어 자동으로 반복 요금이 청구되는 정기 결제의 이름이 '무료 체험판' 또는 '3일간 무료로 프리미엄 멤버십 체험'인 경우가 있습니다.
- 구매 흐름에 여러 화면이 표시되어 사용자가 의도치 않게 정기 결제 버튼을 클릭하게 만듭니다.
- 첫 달에는 보석을 1,000개 제공하고 사용자가 정기 결제를 신청한 후에는 혜택을 보석 1개로 줄이는 사례와 같이 정기 결제에서 지속적이거나 반복적인 가치를 제공하지 않습니다.
- 일회성 혜택을 제공하기 위해 자동 갱신 정기 결제를 신청할 것을 사용자에게 요구하고, 신청 후 사용자의 요청 없이 정기 결제를 취소합니다.

예 1:



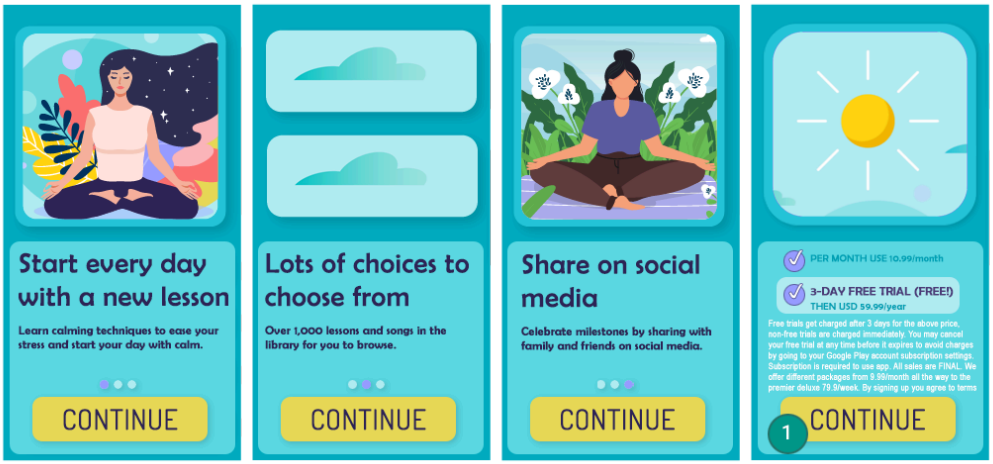
① 닫기 버튼이 명확하게 보이지 않으며 사용자가 정기 결제 혜택을 수락하지 않아도 기능에 액세스할 수 있다는 사실을 알 수 없습니다.

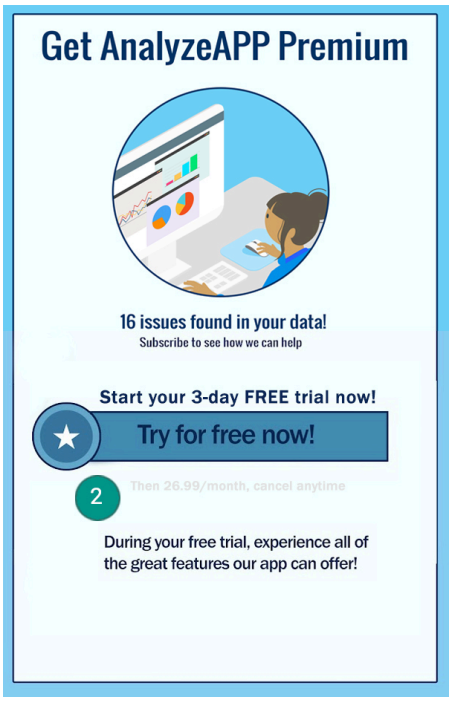
② 혜택에 월별 가격만 표시되어 있어 사용자가 정기 결제를 신청할 때 6개월 가격이 청구된다는 사실을 알 수 없습니다.

③ 혜택에 신규 할인 가격만 표시되어 있어 신규 할인 기간이 종료된 후 어떤 가격이 자동으로 청구되는지 사용자가 알 수 없습니다.

④ 혜택은 사용자가 관련 내용을 모두 이해할 수 있도록 이용약관과 동일한 언어로 현지화되어야 합니다.

예 2:





① 같은 위치의 버튼을 여러 번 클릭하게 하여 사용자가 의도치 않게 '계속' 버튼을 클릭하여 정기 결제를 신청하게 만듭니다.

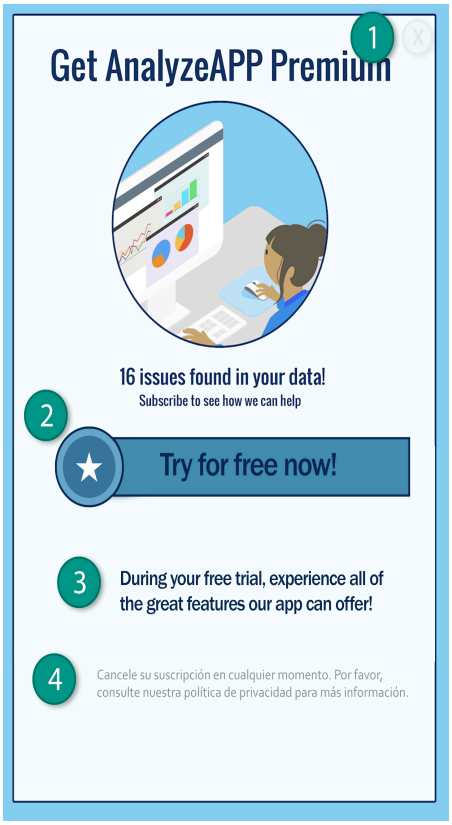
② 무료 체험이 끝난 후 사용자에게 청구되는 요금이 읽기 어려워 사용자가 무료 요금제라고 생각할 수 있습니다.

무료 체험판 및 신규 할인 혜택

사용자가 정기 결제에 등록하기 전: 기간, 가격, 사용 가능한 콘텐츠 또는 서비스 설명 등 혜택의 조건을 명확하고 정확하게 설명해야 합니다. 무료 체험판이 유료 정기 결제로 전환되는 시점과 방식, 유료 정기 결제의 가격, 유료 정기 결제로 전환하고 싶지 않은 경우 정기 결제를 취소할 수 있음을 사용자에게 알려야 합니다.

다음은 자주 발생하는 위반 사례입니다.

- 무료 체험판 기간 또는 신규 할인 가격의 적용 기간을 명확하게 설명하지 않습니다.
- 혜택 기간이 끝나면 유료 정기 결제로 자동 전환된다는 사실을 사용자에게 명확하게 설명하지 않습니다.
- 무료 체험판 없이도 콘텐츠를 사용할 수 있다는 점(가능한 경우)을 명확하게 설명하지 않습니다.
- 현지화가 완료되지 않은 가격 및 약관을 제공합니다.



① 닫기 버튼이 명확하게 보이지 않아서 사용자가 무료 체험판에 가입하지 않아도 기능에 액세스할 수 있다는 사실을 알 수 없습니다.

② 혜택에서 무료 체험판임을 강조해서 사용자는 체험 기간이 종료되면 자동으로 요금이 청구된다는 사실을 알 수 없습니다.

③ 혜택에 체험 기간이 명시되어 있지 않아서 사용자가 정기 결제 콘텐츠에 언제까지 무료로 액세스할 수 있는지 알 수 없습니다.

④ 혜택은 사용자가 관련 내용을 모두 이해할 수 있도록 이용약관과 동일한 언어로 현지화되어야 합니다.

정기 결제 관리, 취소, 환불

앱에서 정기 결제 상품을 판매하는 경우 사용자가 정기 결제를 관리 또는 취소할 수 있는 방법을 앱에 명확하게 공개해야 합니다. 또한 온라인으로 간편하게 정기 결제를 취소하는 방법을 앱에 포함해야 합니다. 앱의 계정 설정 또는 상응하는 페이지에 다음을 포함하여 이 요건을 충족할 수 있습니다.

- Google Play 정기 결제 센터 링크(Google Play 결제 시스템을 사용하는 앱의 경우)
- 개발자의 취소 프로세스에 대한 직접적인 액세스

Google Play 정책에 따르면 사용자가 Google Play 결제 시스템을 통해 구매한 정기 결제를 취소할 경우 현재 결제 기간에 해당하는 요금을 환불받을 수 없지만, 취소일과 관계없이 현재 결제 기간에서 남은 일수 동안 정기 결제 콘텐츠를 계속 이용할 수는 있습니다. 사용자의 정기 결제 취소는 현재 결제 기간이 종료된 후에 적용됩니다.

개발자는 콘텐츠 또는 액세스 제공자로서 사용자에게 더 유연한 환불 정책을 직접 적용할 수 있습니다. 사용자에게 정기 결제, 취소, 환불 정책의 변경사항을 알리고 정책이 관련 법규를 준수하도록 할 의무는 개발자에게 있습니다.

가족용 자체 인증 광고 SDK 프로그램

가족 정책 에 설명된 것처럼 타겟층에 아동만 포함된 앱에 광고를 게재하는 경우 아래의 '가족용 자체 인증 광고 SDK' 요건을 포함해 Google Play 정책을 준수한다고 자체 인증한 광고 SDK 버전만 사용해야 합니다.

앱의 타겟층에 아동과 그 이상의 연령대가 모두 포함되는 경우 아동에게는 자체 인증 광고 SDK 버전 중 하나의 광고만 표시되도록 해야 합니다(예: 중립적인 연령 심사 수단 사용).

'자체 인증 광고 SDK' 버전을 비롯해 앱에 구현하는 모든 SDK 버전이 관련 정책, 현지 법률, 규정을 모두 준수하도록 할 책임은 개발자에게 있습니다. Google에서는 자체 인증 과정에서 광고 SDK가 제공하는 정보의 정확성에 관해 어떠한 진술이나 보증도 하지 않습니다.

'가족용 자체 인증 광고 SDK' 사용은 아동을 대상으로 광고를 게재하는 데 광고 SDK를 사용하는 경우에만 의무사항입니다. 다음과 같은 경우 Google Play를 통한 광고 SDK 자체 인증을 받지 않아도 되지만, 광고 콘텐츠 및 데이터 수집 활동이 Google Play의 사용자 데이터 정책 및 가족 정책 을 준수하도록 할 책임은 개발자에게 있습니다.

- 앱 또는 소유한 기타 미디어의 상호 프로모션과 상품기획을 관리하기 위해 SDK를 사용하는 '인하우스 광고'
- 광고주와 직거래하며 인벤토리 관리용으로 SDK를 사용하는 경우

'가족용 자체 인증 광고 SDK' 요건

- 광고 SDK의 약관 또는 정책에 불쾌감을 주는 광고 콘텐츠 및 행위를 정의하고 이를 금지합니다. 이러한 정의는 'Google Play 개발자 프로그램 정책'을 준수해야 합니다.
- 적절한 연령 그룹에 따라 광고 소재를 평가할 방법을 마련합니다. 적절한 연령 그룹에는 적어도 '전체이용가'와 '미성년자 부적합'은 포함되어야 합니다. 평가 방법은 아래의 신청 양식을 작성한 후 Google이 SDK에 제공하는 방법과 일치해야 합니다.
- 광고 게재와 관련해 게시자가 요청별 또는 앱별로 '아동 대상 서비스로 취급'을 요청할 수 있도록 허용합니다. 이러한 취급은 미국 아동 온라인 개인 정보 보호법(COPPA) 및 EU 개인 정보 보호법(GDPR) 을 포함한 관련 법률 및 규정을 준수하여 이루어져야 합니다. Google Play는 '아동 대상 서비스로 취급'의 일환으로 광고 SDK에서 개인 맞춤 광고, 관심 기반 광고, 리마케팅을 사용 중지할 것을 요구합니다.
- 게시자가 Google Play의 가족 광고 및 수익 창출 정책 을 준수하고 교사 추천 프로그램 의 요건을 충족하는 광고 형식을 선택하도록 허용합니다.
- 아동을 대상으로 광고를 게재하기 위해 실시간 입찰을 사용하는 경우 광고 소재가 검토되고 개인 정보 보호 표시가 입찰자에게 적용되도록 해야 합니다.
- 광고 SDK 정책이 자체 인증 요건을 모두 준수하는지 확인할 수 있도록 아래의 신청 양식 에 명시된 정보와 테스트 앱을 제출하는 등 충분한 정보를 Google에 제공하고, 이후의 정보 요청에도 적시에 응답합니다(예: 새로 출시되는 광고 SDK 버전이 자체 인증 요건을 모두 준수하는지 확인할 수 있도록 새로운 버전 제출 및 테스트 앱 제공).
- 새로 출시되는 모든 버전이 '가족 정책' 요건을 비롯한 최신 'Google Play 개발자 프로그램 정책'을 준수한다는 점을 자체 인증 합니다.

참고: '가족용 자체 인증 광고 SDK'는 게시자에게 적용될 수 있는 아동 관련 법령과 규정을 모두 준수하는 광고 게재 서비스를 지원해야 합니다.

광고 소재의 워터마크 표시 및 테스트 앱 제공에 관한 자세한 정보는 여기 에서 찾을 수 있습니다.

아동을 대상으로 하는 광고를 게재할 때 게재 플랫폼에 적용되는 미디에이션 요건은 다음과 같습니다.

- '가족용 자체 인증 광고 SDK'만 사용하거나 필요한 보호 장치를 구현하여 미디에이션에서 게재된 모든 광고가 이러한 요건을 준수하도록 합니다.
- 광고 콘텐츠 등급 및 '아동 대상 서비스로 취급' 문구(해당하는 경우)를 표시하는 데 필요한 정보를 미디에이션 플랫폼에 보냅니다.

개발자는 여기 에서 '가족용 자체 인증 광고 SDK' 목록과 가족을 위한 앱에 사용할 수 있는 것으로 자체 인증한 광고 SDK의 특정 버전을 확인할 수 있습니다.

또한 자체 인증을 하고자 하는 광고 SDK가 있다면 이 신청 양식 을 공유해 주시기 바랍니다.

스토어 등록정보 및 프로모션

앱의 프로모션 및 조회 가능성은 스토어의 품질에 크게 영향을 미칩니다. 스팸성 스토어 등록정보, 낮은 품질의 프로모션 및 Google Play에서 인위적으로 앱의 조회 가능성을 높이려는 시도는 자제하시기 바랍니다.

앱 프로모션

Google은 사용자 또는 개발자 생태계에 해를 끼치거나, 사용자 또는 개발자를 기만하는 프로모션 관행(예: 광고)에 직간접적으로 관여하거나 이러한 관행을 통해 이익을 취하는 앱을 허용하지 않습니다. 행위 또는 콘텐츠가 개발자 프로그램 정책을 위반하는 경우 프로모션 관행은 사용자를 기만하거나 사용자에게 해를 끼칠 수 있습니다.

다음은 자주 발생하는 위반 사례입니다.

- 시스템 알림, 경고 등과 유사한 알림을 포함하여 웹사이트, 앱, 기타 서비스에서 사기성 광고를 사용하는 행위
- 사용자를 앱의 Google Play 등록정보로 안내하여 앱을 다운로드하게 하기 위해 선정적인 광고를 사용하는 행위
- 사용자가 충분한 정보를 제공받지 않은 상태로 Google Play로 리디렉션되거나 앱을 다운로드하게 하는 프로모션 또는 설치 전략
- SMS 서비스를 통해 요청하지 않은 프로모션을 진행하는 행위
- 스토어 실적 또는 순위, 가격 또는 프로모션 정보를 나타내거나 기존 Google Play 프로그램과의 관계를 시사하는 텍스트 또는 이미지를 앱 제목, 아이콘 또는 개발자 이름에 포함하는 행위

앱과 관련된 모든 광고 네트워크, 제휴사, 광고가 이러한 정책을 준수하게 할 책임은 개발자에게 있습니다.

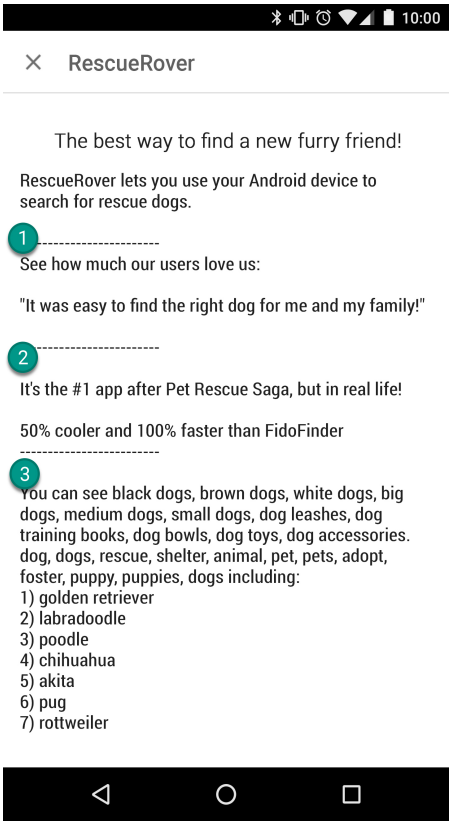
메타데이터

사용자는 앱 설명을 통해 앱의 기능과 목적을 이해합니다. 오해의 소지가 있거나, 잘못된 형식을 사용하거나, 정보를 전달하지 않거나, 관련이 없거나, 과도하거나, 부적절한 메타데이터(앱 설명, 개발자 이름, 제목, 아이콘, 스크린샷, 프로모션 이미지를 포함하되 이에 국한되지 않음)가 포함된 앱은 허용되지 않습니다. 개발자는 앱에 대해 명확하고 잘 작성된 설명을 제공해야 합니다. 앱 설명에 작성자 표기가 없거나 익명인 사용 후기를 포함해서도 안 됩니다.

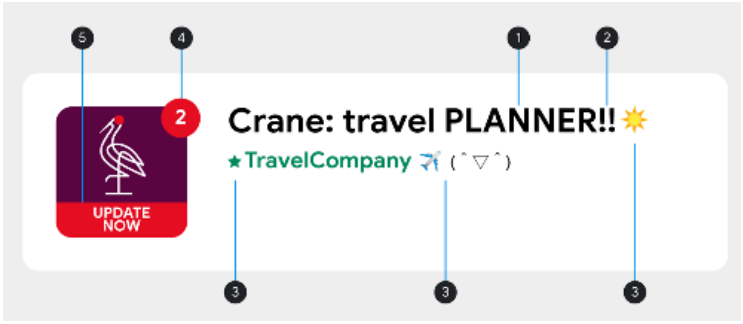
앱 제목, 아이콘 및 개발자 이름은 사용자가 앱을 찾고 앱에 관해 알아보는 데 특히 도움이 됩니다. 메타데이터 요소에 그림 이모티콘, 이모티콘 또는 반복되는 특수문자를 사용하면 안 됩니다. 브랜드 이름의 일부로 쓰인 경우를 제외하면 전체 대문자를 사용하면 안 됩니다. 오해의 소지가 있는 기호가 포함된 앱 아이콘은 허용되지 않습니다(예: 새 메시지가 없는데 새 메시지를 나타내는 점 표시, 앱이 콘텐츠 다운로드와 관련이 없는데 다운로드/설치를 상징하는 기호 사용). 앱 제목은 30자(영문 기준) 이하여야 합니다. 스토어 실적 또는 순위, 가격 또는 프로모션 정보를 나타내거나 기존 Google Play 프로그램과의 관계를 시사하는 텍스트 또는 이미지를 앱 제목, 아이콘 또는 개발자 이름에 포함해서는 안 됩니다.

여기에 언급된 요건 외에도 특정 Google Play 개발자 정책에서 추가 메타데이터 정보를 제공하도록 요구할 수 있습니다.

다음은 자주 발생하는 위반 사례입니다.

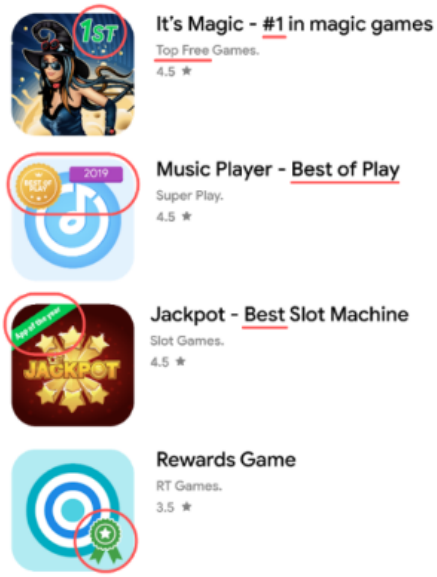


① 작성자 표기가 없거나 익명인 사용 후기
② 앱 또는 브랜드의 데이터 비교
③ 단어 블록 및 세로/가로로 된 단어 목록

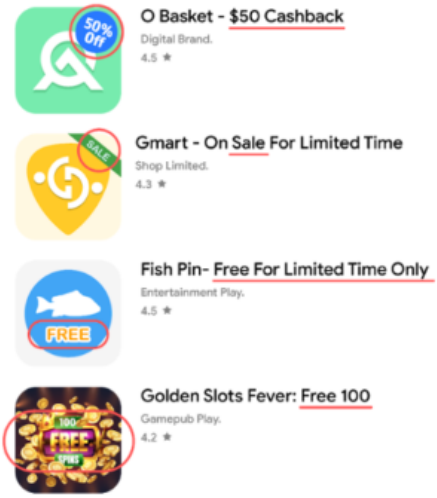


① 브랜드명이 아닌 전체 대문자
② 앱과 관련이 없는 특수문자 반복
③ 그림 이모티콘, 이모티콘(일본 스타일의 이모티콘 포함) 및 특수문자
④ 오해의 소지가 있는 기호
⑤ 오해의 소지가 있는 텍스트

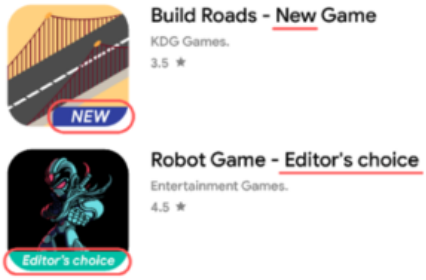
- 스토어 실적 및 순위가 표시된 이미지 또는 텍스트(예: '올해의 앱', '1위', '20XX Play 최고의 앱', '인기', 어워즈 아이콘 등)



- 가격과 홍보 정보가 표시된 이미지 또는 텍스트(예: '10% 할인', '50달러 캐시백', '기간 한정 무료', 등)



- Google Play 프로그램을 나타내는 이미지 또는 텍스트(예: '에디터 추천', '신작' 등)



다음은 등록정보 내의 부적절한 텍스트, 이미지, 동영상의 예입니다.

- 성적인 콘텐츠가 포함된 이미지나 동영상입니다. 그림이든 사진이든 가슴, 엉덩이, 성기, 기타 페티시의 대상이 되는 신체 일부나 콘텐츠가 포함된 성적인 이미지를 사용하지 않도록 하세요.
- 앱의 스토어 등록정보에 욕설이나 저속한 언어 또는 모든 연령대에 적절하지 않은 언어를 사용합니다.
- 앱 아이콘, 프로모션 이미지, 동영상에 폭력이 생생하고 눈에 띄게 묘사되어 있습니다.
- 불법적인 약물 사용이 묘사되어 있습니다. EDSA(교육, 다큐멘터리, 과학, 예술) 콘텐츠인 경우에도 스토어 등록정보 내에는 모든 연령대에 적합한 내용을 표시해야 합니다.

다음은 몇 가지 권장사항입니다.

- 앱의 장점을 강조합니다. 앱과 관련하여 흥미롭고 재미있는 요소를 공유하여 사용자가 앱이 특별한 이유를 인식하도록 돕습니다.

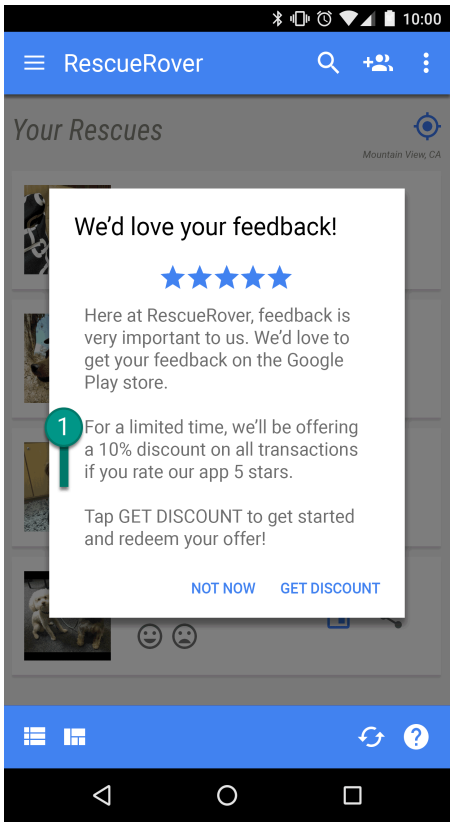
- 앱의 제목과 설명이 앱의 기능을 정확하게 반영하는지 확인합니다.
- 반복적이거나 관련 없는 키워드 또는 참조를 사용하지 않습니다.
- 앱의 설명은 간단명료하게 유지합니다. 특히 화면이 작은 기기에서는 짧은 설명이 더 보기 좋습니다. 지나치게 길거나, 자세하거나, 형식이 부적절하거나, 반복적인 설명은 이 정책에 어긋날 수 있습니다.
- 등록정보는 모든 연령대에 적합해야 한다는 점을 기억하세요. 등록정보에 부적절한 텍스트, 이미지 또는 동영상을 사용하지 않고 위의 가이드라인을 준수합니다.

사용자 평점, 리뷰, 설치 수

개발자는 Google Play에서 앱의 순위를 조작하려고 해서는 안 됩니다. 여기에는 허위 또는 인센티브 제공을 통한 리뷰 및 평점과 같이 부당한 수단을 동원하여 제품 평점, 리뷰 또는 설치 수를 부풀리는 행위 또는 앱의 주요 기능으로 다른 앱을 설치하도록 유도하는 행위가 포함되며 이에 국한되지 않습니다.

다음은 자주 발생하는 위반 사례입니다.

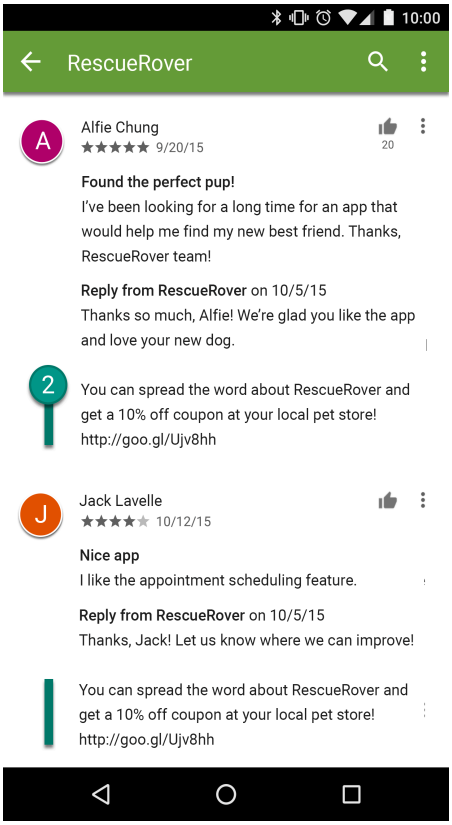
- 사용자에게 인센티브를 제공하고 앱을 평가하도록 요청하는 행위



① 사용자가 높은 평점을 주면 할인을 제공하겠다는 알림

- 사용자로 가장해 반복적으로 평점을 제출하여 Google Play에서 앱의 순위에 영향을 미치는 행위

- 제휴사, 쿠폰, 게임 코드, 이메일 주소, 웹사이트 또는 다른 앱 링크 등 부적절한 콘텐츠를 포함하는 리뷰를 제출하거나 사용자가 제출하도록 조장하는 행위



② 사용자에게 쿠폰 혜택을 이용하여 RescueRover 앱을 홍보할 것을 유도하는 리뷰 내용

평점 및 리뷰는 앱 품질의 기준이 되며 사용자가 앱의 신뢰성 및 관련성을 판단하는 데 사용됩니다. 다음은 사용자 리뷰에 응답할 때 참조할 만한 가이드라인입니다.

- 사용자의 리뷰에서 제기된 실제 문제에 초점을 맞춰야 하며 높은 평점을 요구해서는 안 됩니다.

- 지원 주소나 FAQ 페이지 등 유용한 리소스에 관해 언급합니다.

콘텐츠 등급

Google Play의 콘텐츠 등급은 IARC(International Age Rating Coalition) 에서 제공하며 개발자가 사용자에게 현지 사정에 맞춘 콘텐츠 등급을 알릴 수 있도록 만들어졌습니다. 지역 IARC 당국에서는 앱의 콘텐츠 수위를 결정하기 위한 가이드라인을 마련해 두고 있습니다. Google Play에서는 콘텐츠 등급이 없는 앱이 허용되지 않습니다.

콘텐츠 등급의 용도

콘텐츠 등급은 앱에 불쾌감을 줄 수 있는 콘텐츠가 있음을 소비자(특히 부모)에게 알리는 데 사용됩니다. 또한 법적으로 요구되는 경우 특정 지역 또는 특정 사용자를 대상으로 콘텐츠를 필터링하거나 차단하고, 앱이 특별 개발자 프로그램의 참여 대상인지 결정하는 데도 사용됩니다.

콘텐츠 등급 부여 방법

콘텐츠 등급을 받으려면 앱 콘텐츠의 특성을 묻는 Play Console의 등급 설문지 를 작성해야 합니다. 그러면 여러 등급 부여 기관에서 설문지 답변을 바탕으로 앱에 콘텐츠 등급을 부여하게 됩니다. 앱의 콘텐츠에 관해 허위로 진술하면 앱이 삭제되거나 정지될 수 있으므로 콘텐츠 등급 설문지를 정확하게 작성하는 것이 중요합니다.

앱이 '등급 없음'으로 표시되지 않게 하려면 Play Console에 새로 제출하는 앱은 물론 Google Play에서 제공 중인 기존 앱에 관해서도 모두 콘텐츠 등급 설문지를 작성해야 합니다. 콘텐츠 등급이 없는 앱은 Play 스토어에서 삭제됩니다.

등급 설문지에 입력한 답변에 영향을 미칠 정도로 앱 콘텐츠나 기능을 변경하는 경우, Play Console에서 새로운 콘텐츠 등급 설문지를 제출해야 합니다.

고객센터 를 방문하여 여러 등급 부여 기관 및 콘텐츠 등급 설문지 작성 방법을 자세히 알아보세요.

등급 이의 제기

앱에 부여된 등급에 동의할 수 없다면 인증서 이메일에 있는 링크를 사용하여 IARC 등급 부여 기관에 직접 이의를 제기할 수 있습니다.

뉴스

뉴스 앱은 다음과 같은 앱입니다.

- Google Play Console에서 '뉴스' 앱으로 선언, 또는
- Google Play 스토어의 '뉴스 및 잡지' 카테고리에 표시되어 있고 앱 제목, 아이콘, 개발자 이름 또는 설명에 '뉴스'라고 설명되어 있습니다.

뉴스 앱의 자격이 있으며 '뉴스 및 잡지' 카테고리에 표시되는 앱의 예는 다음과 같습니다.

- 앱 설명에 '뉴스'라고 설명되어 있는 앱으로, 다음을 포함하되 이에 국한되지 않습니다.
  - 최신 뉴스
  - 신문
  - 속보
  - 지역 뉴스
  - 일일 뉴스
- 앱 제목, 아이콘 또는 개발자 이름에 '뉴스'라는 단어가 있는 앱

그러나 주된 내용이 사용자 제작 콘텐츠인 앱(예: 소셜 미디어 앱)은 뉴스 앱으로 선언할 수 없으며 뉴스 앱으로 간주되지 않습니다.

사용자가 멤버십을 구매해야 하는 뉴스 앱은 구매 전에 사용자에게 인앱 콘텐츠 미리보기를 제공해야 합니다.

또한 뉴스 앱은 다음 요건을 충족해야 합니다.

- 앱에 대한 소유권 정보와 뉴스 기사의 출처를 제공해야 합니다. 이는 각 기사의 최초 게시자 또는 작성자를 포함하되 이에 국한되지 않습니다. 기사의 작성자를 개별적으로 명시하는 것이 관례가 아닌 경우 뉴스 앱이 해당 기사의 최초 게시자여야 합니다. 소셜 미디어 계정 링크만으로는 작성자 또는 게시자 정보 요건을 충족할 수 없습니다.
- 연락처 정보를 포함하는 것으로 명확하게 라벨이 지정되어 있고, 찾기 쉬우며(예: 홈페이지 또는 사이트 탐색 메뉴 하단에 링크됨), 뉴스 게시자의 유효한 연락처 정보(연락처 이메일 주소 또는 전화번호 포함)를 제공하는 전용 웹사이트 또는 인앱 페이지가 있어야 합니다. 소셜 미디어 계정 링크만으로는 게시자 연락처 정보 요건을 충족할 수 없습니다.

뉴스 앱에 다음과 같은 문제가 있어서는 안 됩니다.

- 중대한 철자 및/또는 문법 오류가 있으면 안 됩니다.
- 변동사항이 없는 콘텐츠(예: 게시된 지 3개월 이상 지난 콘텐츠)만 포함하면 안 됩니다.
- 주요 목적이 제휴 마케팅 또는 광고 수익 창출이면 안 됩니다.

뉴스 앱은 앱의 주요 목적이 제품 및 서비스의 판매 또는 광고 수익 창출이 아닌 경우에 한하여 수익화를 위해 광고 및 기타 마케팅 방식을 이용하는 것이 *가능합니다*.

여러 게시 출처에서 콘텐츠를 수집하는 뉴스 앱은 앱에 게시되는 콘텐츠의 출처를 투명하게 공개해야 하며 각 출처는 뉴스 정책 요건을 충족해야 합니다.

필요한 정보를 가장 효과적으로 제공하는 방법은 이 도움말을 참고 하세요.

스팸, 기능, 사용자 환경

앱은 몰입도 높은 사용자 환경을 위해 사용자에게 기본적인 수준의 적절한 기능과 콘텐츠를 제공해야 합니다. 다운되거나, 기능 면에서 사용자 환경에 부합하지 않는 기타 동작을 보이거나, 사용자 또는 Google Play에 스팸을 전송하는 것이 유일한 목적인 앱은 유의미한 방식으로 카탈로그를 확장하는 앱이라 볼 수 없습니다.

스팸

사용자 또는 Google Play에 원치 않는 메시지를 보내는 스팸 전송 앱이나 콘텐츠가 중복되거나 품질이 낮은 앱은 허용되지 않습니다.

메시지 스팸

사용자가 콘텐츠와 대상 수신자를 확인할 수 없는 상태에서 사용자 대신 SMS, 이메일 또는 기타 메시지를 보내는 앱은 허용되지 않습니다.

다음은 자주 발생하는 위반 사례입니다.

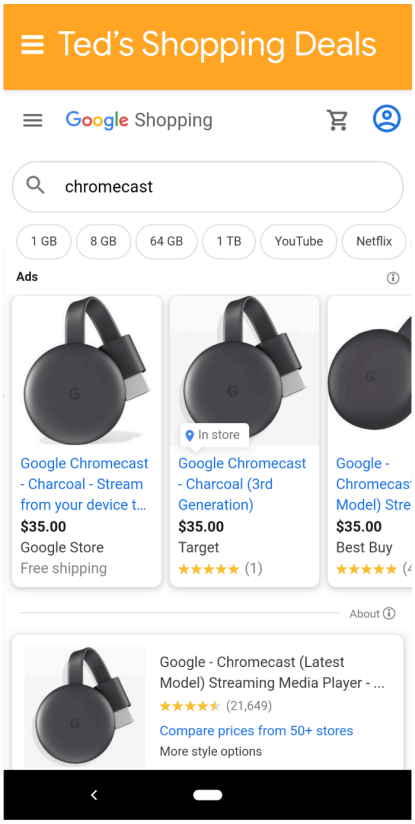
- 사용자가 '공유' 버튼을 누르면 사용자가 내용과 대상 수신자를 확인할 수 없는 상태에서 앱이 사용자를 대신하여 메시지를 전송했습니다.

WebView 및 제휴사 스팸

웹사이트 소유자 또는 관리자의 허가 없이 웹사이트로 제휴사 트래픽을 유도하거나 웹사이트의 WebView를 제공하는 것이 주된 목적인 앱은 허용되지 않습니다.

다음은 자주 발생하는 위반 사례입니다.

- 추천 트래픽을 웹사이트로 유도하여 웹사이트에서의 사용자 로그인 또는 구매에 대한 크레딧을 받는 것이 주목적인 앱
- 다음은 허가 없이 웹사이트의 웹뷰를 제공하는 것이 주요 목적인 앱입니다.



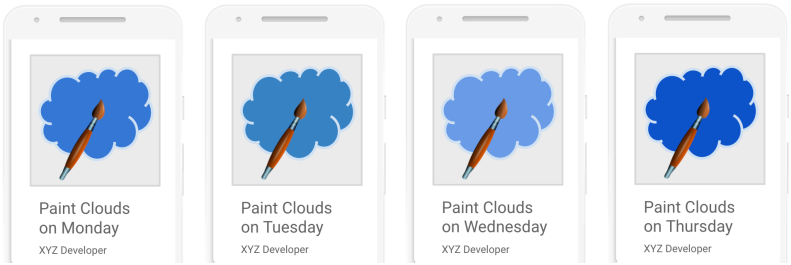
① 앱의 이름은 'Ted's Shopping Deals'인데 단순히 Google 쇼핑의 WebView만 제공합니다.

중복되는 콘텐츠

Google Play에 이미 있는 다른 앱과 동일한 환경을 제공하는 앱은 허용되지 않습니다. 앱은 고유한 콘텐츠 또는 서비스를 제작하여 사용자에게 가치를 제공해야 합니다.

다음은 자주 발생하는 위반 사례입니다.

- 고유한 콘텐츠나 가치를 더하지 않고 다른 앱에서 콘텐츠를 복사합니다.
- 기능, 콘텐츠 및 사용자 환경이 매우 유사한 여러 개의 앱을 제작합니다. 이 경우 각 앱의 콘텐츠 양이 적다면 개발자는 모든 콘텐츠를 모아 하나의 앱을 제작하는 방안을 고려해야 합니다.



기능, 콘텐츠, 사용자 환경

앱은 안정적이고 반응성이 뛰어나며 몰입도가 우수한 사용자 경험을 제공해야 합니다. 앱이 충돌하며 다운되거나, 모바일 앱으로서 기본적인 수준의 적정 활용도를 갖추지 못했거나, 흥미로운 콘텐츠가 부족하거나, 기능적이고 몰입도가 우수한 사용자 경험을 제공하지 않는 등의 다른 행동을 보이는 앱은 Google Play에서 허용되지 않습니다.

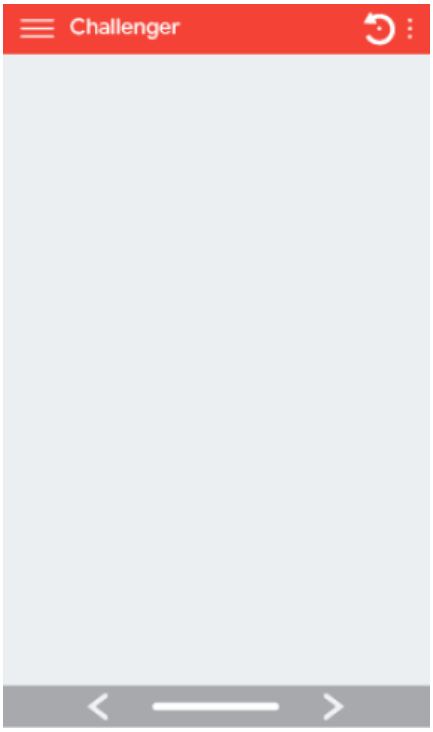
제한된 기능 및 콘텐츠

제한된 기능과 콘텐츠만 있는 앱은 허용되지 않습니다.

다음은 자주 발생하는 위반 사례입니다.

- 특정한 기능 없이 정적인 앱(예: 텍스트 전용 또는 PDF 파일 앱)

- 단일 배경화면 앱과 같이 콘텐츠가 거의 없거나 몰입형 사용자 경험을 제공하지 않는 앱
- 아무 작동 또는 기능도 하지 않도록 설계된 앱

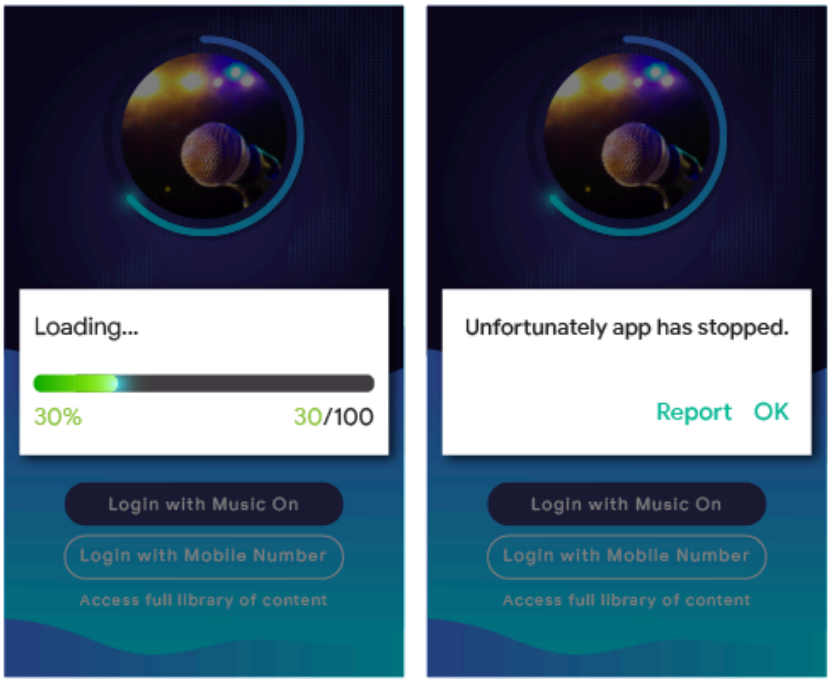


손상된 기능

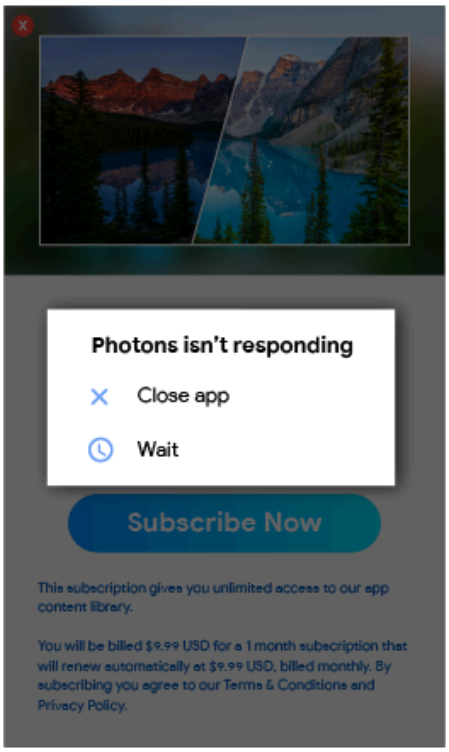
앱이 충돌하며 다운되거나, 강제 종료되거나, 중지되거나, 그 외 비정상적으로 작동하는 앱은 허용되지 않습니다.

다음은 자주 발생하는 위반 사례입니다.

- **설치할 수 없는** 앱
- 설치는 되지만 **로드되지 않는** 앱



- 로드는 되지만 **응답하지 않는** 앱



기타 프로그램

이 정책 센터의 다른 부분에 명시된 콘텐츠 정책을 준수하는 것 외에도 기타 Android 환경을 위해 설계되어 Google Play를 통해 배포되는 앱에는 프로그램별 정책 요구사항이 추가로 적용될 수 있습니다. 아래 목록을 검토하여 이러한 정책이 앱에 적용되는지 확인하시기 바랍니다.

Android 인스턴트 앱

Android 인스턴트 앱의 목표는 쾌적하고 원활한 사용자 환경을 만드는 동시에 높은 수준의 개인정보 보호 및 보안을 유지하는 것입니다. Google 정책은 이러한 목표를 달성할 수 있도록 고안되었습니다.

Google Play를 통해 Android 인스턴트 앱을 배포하기로 한 개발자는 다른 모든 Google Play 개발자 프로그램 정책 외에도 다음 정책을 준수해야 합니다.

ID

로그인 기능이 있는 인스턴트 앱의 경우 개발자는 비밀번호 대용 Smart Lock 을 통합해야 합니다.

링크 지원

Android 인스턴트 앱 개발자는 다른 앱의 링크를 올바르게 지원해야 합니다. 개발자의 인스턴트 앱이나 설치된 앱에 인스턴트 앱으로 연결될 수도 있는 링크가 포함된 경우, 개발자는 WebView 를 통해 링크로 연결하는 등의 방법을 사용하는 대신 해당 인스턴트 앱으로 사용자를 연결해야 합니다.

기술 사양

개발자는 공개 도움말 에 명시된 내용을 포함하여 Google에서 제공하는 Android 인스턴트 앱 기술 사양과 요구사항을 충족해야 합니다. 이러한 사양과 요구사항은 수시로 변경될 수 있습니다.

앱 설치 제공

인스턴트 앱은 사용자에게 설치 가능한 앱을 제공할 수 있으나, 이것이 인스턴트 앱의 주목적이 되어서는 안 됩니다. 개발자는 앱 설치를 제공할 때 다음을 준수해야 합니다.

- 머티리얼 디자인이 적용된 '앱 다운로드' 아이콘 과 '설치' 라벨을 설치 버튼으로 사용합니다.
- 인스턴트 앱에 간접적으로 설치를 유도하는 메시지를 2~3개 이상 포함하지 않습니다.
- 사용자에게 설치 유도 메시지를 표시할 때 배너 등 광고와 유사한 기술을 사용하지 않습니다.

인스턴트 앱에 관한 추가 정보와 UX 가이드라인은 사용자 환경 권장사항 에서 확인하세요.

기기 상태 변경

인스턴트 앱은 인스턴트 앱 세션보다 오래 지속되는 변경사항을 사용자 기기에 적용해서는 안 됩니다. 예를 들어, 인스턴트 앱은 사용자의 배경화면을 변경하거나 홈 화면 위젯을 생성할 수 없습니다.

앱 표시 여부

개발자는 사용자가 기기에서 인스턴트 앱이 실행 중이라는 것을 항상 알 수 있도록 인스턴트 앱을 표시해야 합니다.

기기 식별자

인스턴트 앱은 (1) 인스턴트 앱의 실행이 중지된 후에도 지속되고 (2) 사용자가 재설정할 수 없는 기기 식별자에 액세스할 수 없습니다. 여기에 해당하는 대표적인 예는 다음과 같습니다.

- Build Serial
- 네트워크 칩의 MAC 주소
- IMEI, IMSI

인스턴트 앱은 런타임 권한을 사용하여 전화번호에 액세스할 수 있습니다. 개발자는 이러한 식별자나 다른 수단을 사용하여 사용자를 식별해서는 안 됩니다.

네트워크 트래픽

인스턴트 앱 내의 네트워크 트래픽은 HTTPS와 같은 TLS 프로토콜을 사용하여 암호화해야 합니다.

Android 그림 이모티콘 정책

Google의 그림 이모티콘 정책은 포용적이고 일관된 사용자 환경을 촉진하기 위해 고안되었습니다. 이를 위해 Android 12 이상에서 실행되는 모든 앱은 최신 버전의 유니코드 그림 이모티콘 을 지원해야 합니다.

맞춤 구현 없이 기본 Android 그림 이모티콘을 사용하는 앱은 Android 12 이상에서 실행 시 이미 최신 버전의 유니코드 그림 이모티콘을 사용하고 있습니다.

타사 라이브러리에서 제공하는 그림 이모티콘을 비롯해 그림 이모티콘을 맞춤 구현한 앱은 Android 12 이상에서 실행 시 새 유니코드 그림 이모티콘 출시 후 4개월 이내에 최신 유니코드 버전을 완전히 지원해야 합니다.

최신 그림 이모티콘 지원 방법은 이 가이드 를 참고하세요.

가족

Google Play는 개발자가 온 가족의 연령대에 적합한 양질의 콘텐츠를 선보일 수 있도록 풍부한 플랫폼을 제공합니다. 개발자에게는 가족을 위한 앱 프로그램에 앱을 제출하거나 어린이를 대상으로 하는 앱을 Google Play 스토어에 제출하기 전에 앱이 어린이에게 적합하며 관련 법률을 모두 준수하는지 확인할 책임이 있습니다.

앱 개발자 아카데미에서 가족 정책 요구사항에 관해 알아보고 대화형 체크리스트를 검토해 보세요.

Google Play 가족 정책

기술을 가족의 삶을 풍요롭게 하는 도구로 사용하는 경향이 계속 증가하고 있으며, 부모들은 자녀와 공유할 수 있는 안전하며 우수한 콘텐츠를 찾고 있습니다. 아동을 대상으로 하는 앱을 설계하고 있을 수도 있고, 의도하지 않더라도

내 앱이 아동의 관심을 끌게 될 수도 있습니다. Google Play는 개발자의 앱이 가족을 포함한 모든 사용자에게 안전한 앱이 될 수 있도록 도움이 되고자 합니다.

'아동'이라는 단어는 언어와 상황에 따라 서로 다른 대상을 의미할 수 있습니다. 법률 전문가의 도움을 받아 앱에 적용될 수 있는 의무사항 또는 연령에 따른 제한사항을 확인해야 합니다. 앱이 어떻게 작동하는지는 개발자가 가장 잘 알고 있으므로 Google은 개발자의 도움을 받아 Google Play 앱이 가족용 콘텐츠임을 확인하고 있습니다.

Google Play 가족 정책을 준수하는 모든 앱은 교사 추천 프로그램을 위한 평가를 받도록 선택할 수 있으나, 평가를 받는다고 해서 앱이 교사 추천 프로그램에 포함된다는 보장은 없습니다.

Play Console 요구사항

타겟층 및 콘텐츠

앱을 게시하기 전에 Google Play Console의 타겟층 및 콘텐츠 섹션에 제공된 목록에서 연령대를 선택하여 앱의 타겟층을 지정해야 합니다. Google Play Console에서 지정한 내용과 관계없이 어린이를 대상으로 하는 앱처럼 간주될 수 있는 이미지와 용어를 앱에 포함하면 Google Play에 신고된 타겟층을 평가하는 데 영향을 미칠 수 있습니다. Google Play는 공개하는 타겟층이 정확한지 판단하기 위해 제공한 앱 정보를 자체적으로 검토할 권리를 보유합니다.

일부 연령대를 대상으로 앱을 설계하였으며 앱이 관련 연령대에 속한 사용자에게 적절하다고 생각한다면 앱의 타겟층으로 둘 이상의 연령대만 선택해야 합니다. 예: 영아, 유아, 미취학 어린이를 대상으로 설계한 앱은 대상 연령대로 '만 5세 이하'만 선택해야 합니다. 특정 학년을 대상으로 앱을 개발했다면 그 학년에 가장 적합한 연령대를 선택합니다. 모든 연령을 대상으로 앱을 설계한 경우에만 성인과 아동을 모두 포함하는 연령대를 선택해야 합니다.

타겟층 및 콘텐츠 섹션 업데이트

Google Play Console의 타겟층 및 콘텐츠 섹션에서 앱 정보를 언제든 업데이트할 수 있습니다. 이 정보가 Google Play 스토어에 반영되려면 앱 업데이트 가 필요합니다. 단, Google Play Console의 타겟층 및 콘텐츠 섹션에서 변경한 사항은 앱 업데이트를 제출하기 전에도 정책 준수 여부를 검토받을 수 있습니다.

앱의 대상 연령대를 변경하거나 광고 또는 인앱 구매를 사용하기 시작하려면 앱의 스토어 등록정보 페이지에서 '변경사항' 섹션을 사용하거나 인앱 알림을 통해 기존 사용자에게 알리는 것이 좋습니다.

Play Console의 허위 정보

타겟층 및 콘텐츠 섹션을 포함하여 Play Console에 게재된 앱에 관한 허위 정보가 있으면 앱이 삭제 또는 정지될 수 있으므로 정확한 정보를 제공하는 것이 중요합니다.

가족 정책 요구사항

앱의 타겟층 중 하나가 아동인 경우 다음 요건을 준수해야 합니다. 이러한 요건을 충족하지 않으면 앱이 삭제 또는 정지될 수 있습니다.

1. **앱 콘텐츠:** 아동이 이용할 수 있는 앱 콘텐츠는 아동에게 적합해야 합니다. 앱에 포함된 콘텐츠가 전 세계 공통으로 적절한 것은 아니나 특정 지역에서는 아동 사용자에게 적절하다고 간주되는 경우 해당 지역(제한된 지역)에서는 앱이 제공될 수 있으나 그 외의 지역에서는 제공되지 않습니다.
2. **앱 기능:** 웹사이트 소유자 또는 관리자의 허가 없이 앱이 단순히 웹사이트의 웹뷰만 제공하거나 앱의 주목적이 제휴사 트래픽을 웹사이트로 유도하는 것이어서는 안 됩니다.
3. **Play Console 답변:** Play Console에서 앱에 관한 질문에 정확하게 답변하고 앱에 변경사항이 있는 경우 이를 정확하게 반영하도록 답변을 업데이트해야 합니다. 이는 타겟층 및 콘텐츠 섹션, 데이터 보안 섹션, IARC 콘텐츠 등급 설문지에서 앱에 관해 정확한 응답을 제공하는 것을 포함하되 이에 국한되지 않습니다.
4. **데이터 관행:** 앱에서 API와 SDK를 호출 또는 사용하여 정보를 수집하는 경우를 포함해 아동으로부터 개인 정보와 민감한 정보를 수집하는 경우 수집 사실을 반드시 공개해야 합니다. 아동의 민감한 정보는 인증 정보, 마이크 및 카메라 센서 데이터, 기기 데이터, Android ID, 광고 사용 데이터를 포함하되 이에 국한되지 않습니다. 또한 앱이 아래의 데이터 관행을 준수하도록 해야 합니다.
   - 아동만을 타겟팅하는 앱은 Android 광고 ID(AAID), SIM 일련번호, 빌드 일련번호, BSSID, MAC, SSID, IMEI 및/또는 IMSI를 전송해서는 안 됩니다.
     - 아동만을 타겟팅하는 앱은 Android API 33 이상을 타겟팅할 때 AD_ID 권한을 요청해서는 안 됩니다.

- 아동과 그 이상의 연령대를 모두 타겟팅하는 앱은 아동 또는 연령 미상인 사용자의 AAID, SIM 일련번호, 빌드 일련번호, BSSID, MAC, SSID, IMEI 및/또는 IMSI를 전송해서는 안 됩니다.
- Android API의 TelephonyManager에서 기기 전화번호를 요청해서는 안 됩니다.
- 아동만을 타겟팅하는 앱은 위치 정보 액세스 권한을 요청하거나 정확한 위치를 수집, 사용, 전송해서는 안 됩니다.
- 앱이 부속 기기 관리자(CDM) 와 호환되지 않는 기기 운영체제(OS) 버전만 타겟팅하는 경우가 아니라면, 블루투스를 요청할 때는 항상 CDM을 사용해야 합니다.

5. **API와 SDK:** 앱에서 모든 API와 SDK를 제대로 구현하는지 확인해야 합니다.
   - 아동만을 타겟팅하는 앱에는 아동이 주요 대상인 서비스에 사용하도록 승인되지 않은 API 또는 SDK를 포함해서는 안 됩니다.
     - 인증 및 승인에 OAuth 기술을 사용하며 서비스 약관에서 아동 대상 서비스에 사용하도록 승인되지 않았음을 명시하는 API 서비스를 예로 들 수 있습니다.
   - 아동과 그 이상의 연령대를 모두 타겟팅하는 앱은 중립적인 연령 심사를 거치거나 아동으로부터 데이터를 수집하지 않는 방식으로 구현하지 않는 한 아동을 대상으로 한 서비스에 사용하도록 승인되지 않은 API나 SDK를 구현해서는 안 됩니다. 아동과 그 이상의 연령대를 모두 타겟팅하는 앱은 사용자가 아동 대상 서비스에 사용하도록 승인되지 않은 API 또는 SDK를 통해 앱 콘텐츠에 액세스하도록 요구해서는 안 됩니다.

6. **증강 현실(AR):** 앱에서 증강 현실을 사용하는 경우 AR 섹션을 실행하는 즉시 안전 경고를 제공해야 합니다. 경고에는 다음 내용이 포함되어야 합니다.
   - 부모 감독 기능의 중요성을 언급하는 적절한 메시지가 있어야 합니다.
   - 실제 환경에서 발생할 수 있는 신체적 위험에 주의하라는 알림(예: 주변 환경에 유의)이 있어야 합니다.
   - 앱에서 Daydream, Oculus 등 아동의 사용이 권장되지 않는 기기 사용을 요구해서는 안 됩니다.

7. **소셜 애플리케이션 및 기능:** 앱에서 사용자가 정보를 공유하거나 교환하도록 허용하는 경우 Play Console의 콘텐츠 등급 설문지에 이러한 기능을 정확하게 공개해야 합니다.
   - 소셜 애플리케이션: 소셜 애플리케이션은 사용자가 자유 형식의 콘텐츠를 공유하거나 많은 사람과 소통할 수 있도록 지원하는 데 중점을 두는 앱입니다. 타겟층에 아동이 포함된 모든 소셜 애플리케이션은 아동 사용자가 자유 형식의 미디어 또는 정보를 교환할 수 있도록 허용하기 전에 안전하게 인터넷을 사용하고 현실 세계에 온라인 상호작용이 미칠 수 있는 위험을 인식하도록 인앱 알림을 제공해야 합니다. 또한 아동 사용자가 개인 정보를 교환할 수 있는 기능을 허용하려면 사전에 성인 인증을 요구해야 합니다.
   - 소셜 기능: 소셜 기능은 사용자가 자유 형식의 콘텐츠를 공유하거나 많은 사람과 소통할 수 있도록 지원하는 추가 앱 기능입니다. 타겟층에 아동이 포함되어 있으며 소셜 기능이 있는 모든 앱은 아동 사용자가 자유 형식의 미디어 또는 정보를 교환할 수 있도록 허용하기 전에 안전하게 인터넷을 사용하고 현실 세계에 온라인 상호작용이 미칠 수 있는 위험을 인식하도록 인앱 알림을 제공해야 합니다. 또한 소셜 기능을 사용 설정/중지하거나 기능의 수준을 선택하는 방식을 포함하되 이에 국한되지 않는 방법으로 보호자가 아동 사용자를 위해 소셜 기능을 관리할 수 있는 수단을 제공해야 합니다. 마지막으로, 아동의 개인 정보 교환을 허용하는 기능을 사용 설정하려면 사전에 성인 인증을 요구해야 합니다.
   - 성인 인증은 사용자가 아동이 아니며 아동이 성인용으로 설계된 앱 영역에 액세스하기 위해 연령을 속이도록 조장하지 않았음을 증명하는 메커니즘을 의미합니다(즉, 성인 PIN, 비밀번호, 생년월일, 이메일 인증, 사진이 부착된 신분증, 신용카드, 사회보장번호(SSN)).
   - 모르는 사람과 채팅하는 데 중점을 둔 소셜 애플리케이션은 아동을 타겟팅해서는 안 됩니다. 예를 들면 채팅 룰렛 스타일 앱, 데이트 앱, 아동 중심의 공개 채팅방 등이 있습니다.

8. **법률 준수:** 앱에서 호출하거나 사용하는 모든 API 또는 SDK를 포함해 앱이 미국 아동 온라인 개인 정보 보호법(COPPA) , EU 개인 정보 보호법(GDPR) , 기타 관련 법규 또는 규정을 준수하도록 해야 합니다.

다음은 자주 발생하는 위반 사례입니다.

- 스토어 등록정보에서 아동용 앱이라고 홍보하지만 앱 콘텐츠가 성인 전용인 앱
- 서비스 약관에 따라 아동 대상 앱에서 사용이 금지된 API가 구현된 앱
- 주류, 담배 또는 규제 약물의 사용을 미화하는 앱
- 실제 도박 또는 시뮬레이션 도박이 포함된 앱
- 아동에게 적합하지 않은 폭력, 유혈 장면 또는 충격적인 콘텐츠가 포함된 앱
- 데이트 서비스를 제공하거나 성적인 조언 또는 부부생활 관련 조언을 제공하는 앱

- Google Play의 개발자 프로그램 정책 을 위반하는 콘텐츠가 표시되는 웹사이트의 링크가 포함된 앱
- 아동에게 성인 광고(예: 폭력적인 콘텐츠, 성적인 콘텐츠, 도박 콘텐츠)를 표시하는 앱

광고 및 수익 창출

Play에서 아동을 대상으로 하는 앱으로 수익을 창출하는 경우 앱이 다음 가족용 광고 및 수익 창출 정책 요구사항을 준수해야 합니다.

아래 정책은 광고, 내 앱과 타사 앱의 상호 프로모션, 인앱 구매 혜택 또는 기타 모든 상업적 콘텐츠(예: 유료 PPL)를 포함한 모든 수익 창출 및 광고에 적용됩니다. 이러한 앱의 모든 수익 창출 및 광고는 모든 관련 법률 및 규정(관련 자체 규제 또는 업계 가이드라인 포함)을 준수해야 합니다.

Google Play는 과도하게 공격적인 상업 전략을 이유로 앱을 거부, 삭제 또는 정지할 권리를 보유합니다.

광고 요건

앱이 아동 또는 연령을 알 수 없는 사용자에게 광고를 표시하는 경우 다음 사항을 준수해야 합니다.

- 해당 사용자에게 광고를 표시하려면 Google Play 가족용 자체 인증 광고 SDK만 사용해야 합니다.
- 해당 사용자에게 표시되는 광고는 관심 기반 광고(온라인 탐색 행동을 기준으로 특정한 특성을 가진 개별 사용자를 타겟팅하는 광고) 또는 리마케팅(앱 또는 웹사이트와의 이전 상호작용을 기준으로 개별 사용자를 타겟팅하는 광고)을 포함하지 않아야 합니다.
- 해당 사용자에게 표시되는 광고는 아동에게 적합한 콘텐츠를 제공해야 합니다.
- 해당 사용자에게 표시되는 광고는 가족 광고 형식 요건을 준수해야 합니다.
- 아동 대상 광고와 관련된 법률 규정 및 업계 표준을 모두 준수해야 합니다.

광고 형식별 요건

앱의 수익 창출 및 광고는 사기성 콘텐츠를 포함하거나 아동 사용자의 의도하지 않은 클릭을 유도하는 방식으로 설계되어서는 안 됩니다.

다음은 앱의 유일한 타겟층이 아동인 경우 금지되는 사항입니다. 앱의 타겟층이 아동과 그 이상의 연령대인 경우에도 아동 또는 연령 미상의 사용자를 대상으로 광고를 게재한다면 다음 사항은 금지됩니다.

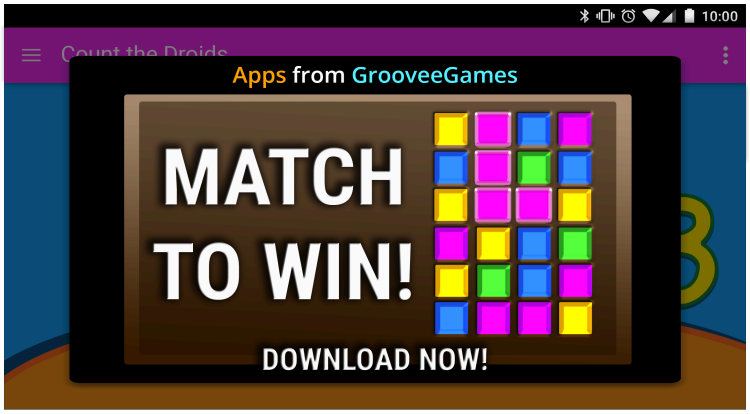
- 전체 화면을 차지하거나 정상적인 앱 사용을 방해하고 명확한 광고 닫기 수단을 제공하지 않는 수익 창출 및 광고를 포함하여 불편을 야기하는 수익 창출 및 광고(예: 광고 벽)
- 5초 후에도 닫을 수 없는 보상형 광고나 수신 동의 광고를 포함하여 정상적인 앱 사용 또는 게임플레이를 방해하는 수익 창출 및 광고
- 정상적인 앱 사용 또는 게임플레이를 방해하지 않는 수익 창출 및 광고(예: 광고가 통합된 동영상 콘텐츠)는 5초 이상 지속될 수 있음
- 앱이 시작되는 즉시 표시되는 전면 수익 창출 및 광고
- 한 페이지 내 여러 위치에 게재되는 광고(예: 하나의 게재위치에 여러 가지를 광고하는 배너 광고나 둘 이상의 배너 또는 동영상 광고를 표시하는 행위는 허용되지 않음)
- Offerwall 및 기타 몰입형 광고 경험 등 앱 콘텐츠와 명확하게 구분되지 않는 수익 창출 및 광고
- 광고 시청 또는 인앱 구매를 유도하기 위해 충격을 주거나 감정을 조종하는 전략 사용
- 다른 광고가 트리거되는 닫기 버튼을 사용하거나 다른 기능을 위해 사용자가 자주 탭하는 앱 영역에 갑자기 광고를 표시하여 사용자가 클릭하도록 하는 사기성 광고
- 인앱 구매 시 가상의 게임 코인 사용과 실제 현금 사용 간에 차이를 두지 않음

다음은 자주 발생하는 위반 사례입니다.

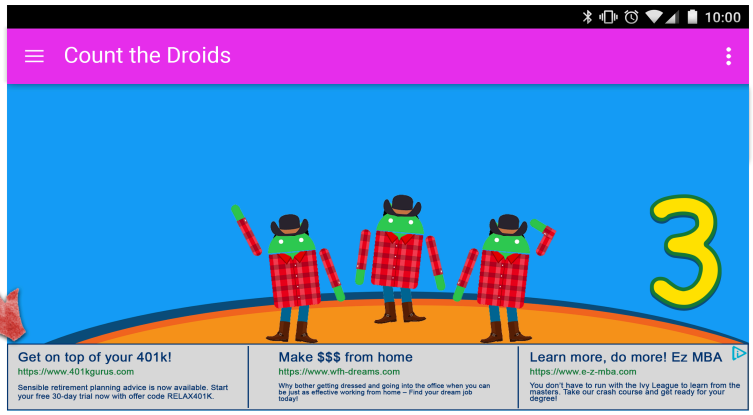
- 사용자가 광고를 닫으려고 하면 사용자의 손가락에서 멀어지는 수익 창출 및 광고

- 아래 예와 같이 사용자에게 5초가 지난 후에도 혜택을 종료할 수 있는 방법을 제공하지 않는 수익 창출 및 광고

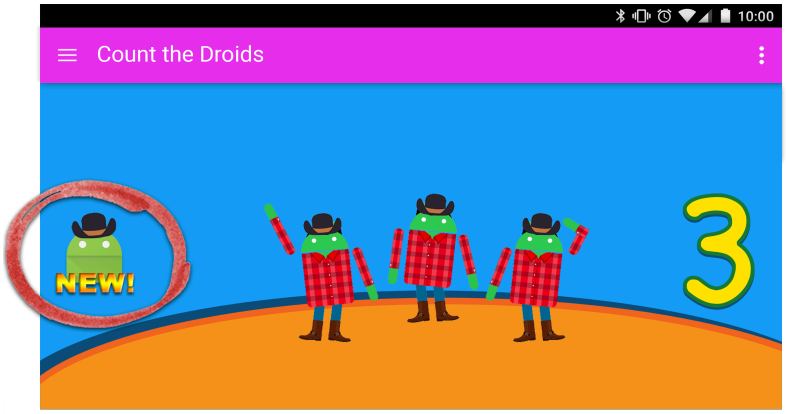
- 아래 예와 같이 기기 화면 대부분을 차지하면서 사용자가 닫을 수 있는 명확한 방법을 제시하지 않는 수익 창출 및 광고



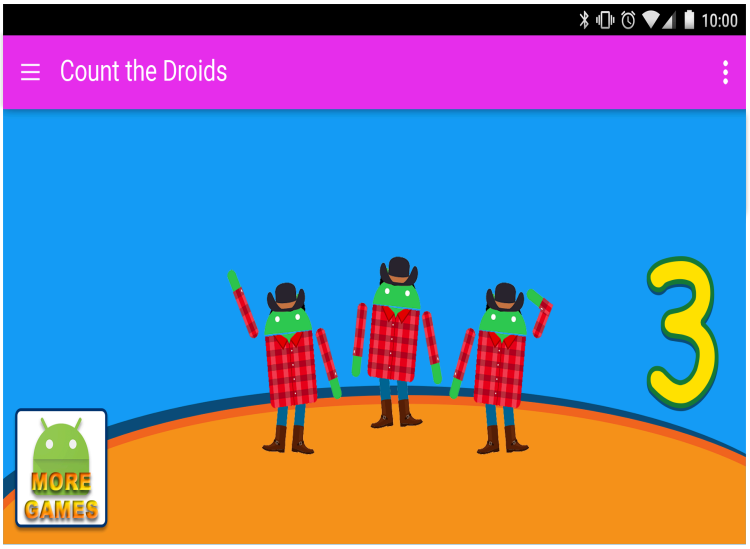
- 아래 예와 같이 여러 개의 혜택이 표시되는 배너 광고



- 아래 예와 같이 사용자가 앱 콘텐츠로 오인할 수 있는 수익 창출 및 광고



- 아래 예와 같이 다른 Google Play 스토어 등록정보를 홍보하지만, 앱 콘텐츠와 구별할 수 없는 버튼, 광고 또는 기타 수익 창출



다음은 아동에게 표시해서는 안 되는 부적절한 광고 콘텐츠의 예입니다.

- **부적절한 미디어 콘텐츠**: 아동에게 부적합한 TV 프로그램, 영화, 음악 앨범 또는 기타 미디어 매체에 관한 광고
- **부적절한 비디오 게임 및 다운로드 가능 소프트웨어**: 아동에게 적합하지 않은 다운로드 가능한 소프트웨어와 전자 비디오 게임에 관한 광고
- **규제 약물 또는 유해 물질**: 주류, 담배, 규제 약물 또는 기타 유해 물질의 광고
- **도박**: 시뮬레이션된 도박이나 콘테스트, 경품 행사 프로모션에 대한 광고(무료 참여 가능해도 허용되지 않음)
- **성인용 및 선정적 콘텐츠**: 성적, 선정적이거나 미성년자 부적합 콘텐츠가 포함된 광고
- **데이트 또는 교제**: 데이트 또는 성인 교제 사이트 광고
- **폭력적인 콘텐츠**: 아동에게 부적합한 폭력적이고 노골적인 콘텐츠가 묘사된 광고

광고 SDK

타겟층에 아동만 포함된 앱에 광고를 게재할 경우 가족용 자체 인증 광고 SDK 버전만 사용해야 합니다. 앱의 타겟층에 아동과 그 이상의 연령대 사용자가 모두 포함되는 경우에는 중립적인 연령 심사 와 같은 연령 심사 수단을 구현하고 아동에게는 Google Play 자체 인증 광고 SDK 버전에 해당하는 광고만 표시되도록 해야 합니다.

이러한 요건에 관한 자세한 내용은 가족용 자체 인증 광고 SDK 프로그램 정책 페이지를 참고하고 여기 에서 '가족용 자체 인증 광고 SDK' 버전의 최신 목록을 확인하세요.

AdMob을 사용하는 경우 AdMob 고객센터 에서 제품에 관한 자세한 내용을 확인하시기 바랍니다.

앱이 광고, 인앱 구매, 상업적 콘텐츠와 관련된 요건을 모두 충족하도록 할 책임은 개발자에게 있습니다. 콘텐츠 정책 및 광고 권장사항에 관해 자세히 알아보려면 광고 SDK 제공업체에 문의하세요.

가족용 자체 인증 광고 SDK 정책

Google Play는 아동과 가족에게 안전한 환경을 만들기 위해 최선을 다하며, 특히 아동에게 연령에 적합한 광고만 표시하고 아동의 데이터를 적절하게 취급하는 데 주력하고 있습니다. 이러한 목표를 달성하기 위해 광고 SDK 및 미디에이션 플랫폼이 아동에게 적합하며 Google Play 개발자 프로그램 정책 및 가족용 자체 인증 광고 SDK 프로그램 요건 을 포함한 Google Play 가족 정책 을 준수함을 자체 인증할 것을 요구하고 있습니다.

Google Play '가족용 자체 인증 광고 SDK 프로그램'은 아동용으로 설계된 앱에 사용하기 적합한 것으로 자체 인증한 광고 SDK 또는 미디에이션 플랫폼을 개발자가 식별할 수 있는 중요한 방법입니다.

신청 양식 등에 SDK에 관한 허위 정보가 있으면 '가족용 자체 인증 광고 SDK 프로그램'에서 SDK가 삭제 또는 정지될 수 있으므로 정확한 정보를 제공해야 합니다.

정책 요건

SDK 또는 미디에이션 플랫폼에서 Google Play 가족을 위한 앱 프로그램에 참여하는 앱에 광고를 게재하는 경우 개발자는 다음 요건을 포함해 'Google Play 개발자 정책'을 모두 준수해야 합니다. 정책 요건을 충족하지 않으면 가족용 자체 인증 광고 SDK 프로그램에서 삭제되거나 정지될 수 있습니다.

SDK 또는 미디에이션 플랫폼이 규정을 준수하도록 할 책임은 개발자에게 있으므로 Google Play 개발자 프로그램 정책, Google Play 가족 정책, 가족용 자체 인증 광고 SDK 프로그램 요건을 검토하시기 바랍니다.

1. **광고 콘텐츠:** 아동이 이용할 수 있는 광고 콘텐츠는 아동에게 적합해야 합니다.
   - 약관 또는 정책에 (i) 불쾌감을 주는 광고 콘텐츠 및 행위를 정의하고 (ii) 이를 금지해야 합니다. 이러한 정의는 Google Play 개발자 프로그램 정책에 부합해야 합니다.
   - 적절한 연령대에 따라 광고 소재의 등급을 지정할 방법도 마련해야 합니다. 적절한 연령대에는 적어도 '전체이용가'와 '성인용'이 포함되어야 합니다. 등급을 지정하는 방법은 신청 양식 을 작성한 후에 Google이 SDK에 제공하는 방법과 일관성이 있어야 합니다.
   - 아동을 대상으로 광고를 게재하기 위해 실시간 입찰을 사용하는 경우 광고 소재를 검토하고 위의 요건을 준수하도록 해야 합니다.
   - 또한 인벤토리에 게재되는 광고 소재를 시각적으로 식별하는 메커니즘을 마련해야 합니다(예: 회사의 시각적 로고로 광고 소재에 워터마크를 표시하는 기능 등).
2. **광고 형식:** 아동 사용자에게 표시되는 모든 광고가 가족 광고 형식별 요건을 준수하도록 해야 하며, 개발자가 Google Play 가족 정책을 준수하는 광고 형식을 선택할 수 있도록 허용해야 합니다.
   - 광고는 사기성 콘텐츠를 포함하거나 아동 사용자의 의도하지 않은 클릭을 유도하는 방식으로 설계되어서는 안 됩니다. 다른 광고가 트리거되는 닫기 버튼을 사용하거나, 다른 기능을 위해 사용자가 자주 탭하는 앱 영역에 갑자기 광고를 표시하여 사용자가 클릭하도록 하는 사기성 광고는 허용되지 않습니다.
   - 전체 화면을 가리거나 정상적인 앱 사용을 방해하며 광고를 닫을 수 있는 명확한 수단을 제공하지 않는 광고(예: 광고 벽) 등 앱 경험을 방해하는 광고는 허용되지 않습니다.
   - 보상형 광고나 수신 동의 광고 등 정상적인 앱 사용 또는 게임 플레이를 방해하는 광고는 5초 후 닫을 수 있어야 합니다.
   - 한 페이지의 여러 위치에 광고를 게재하는 것은 허용되지 않습니다. 예를 들어 하나의 게재위치에 여러 내용을 광고하는 배너 광고나 둘 이상의 배너 또는 동영상 광고를 표시하는 것은 허용되지 않습니다.
   - 광고는 앱 콘텐츠와 명확하게 구분되어야 합니다. 아동 사용자가 분명하게 광고로 식별할 수 없는 Offerwall 및 몰입형 광고 경험은 허용되지 않습니다.
   - 광고는 광고 시청을 유도하기 위해 충격을 주거나 감정을 조종하는 전략을 사용해서는 안 됩니다.
3. **관심 기반 광고/리마케팅:** 아동 사용자에게 표시되는 광고에는 관심 기반 광고(온라인 탐색 행동을 기준으로 특정한 특성을 가진 개별 사용자를 타겟팅하는 광고) 또는 리마케팅(앱 또는 웹사이트와의 이전 상호작용을 기준으로 개별 사용자를 타겟팅하는 광고)이 포함되지 않도록 해야 합니다.
4. **데이터 관행:** SDK 제공업체는 사용자 데이터(예: 기기 정보를 포함해 사용자로부터 또는 사용자에 관해 수집하는 정보) 처리 방식을 투명하게 밝혀야 합니다. 이는 SDK의 데이터 액세스, 수집, 사용, 공유 정보를 공개하고 데이터의 용도를 공개된 목적으로 제한해야 한다는 의미입니다. 이러한 Google Play 요건은 관련 개인 정보 보호법 및 데이터 보호법에 규정된 요건에 추가로 적용됩니다. 아동으로부터 인증 정보, 마이크 및 카메라 센서 데이

터, 기기 데이터, Android ID, 광고 사용 데이터를 포함하되 이에 국한되지 않는 개인 정보와 민감한 정보를 수집하는 경우 수집 사실을 반드시 공개해야 합니다.

- 광고 게재와 관련해 개발자가 요청별 또는 앱별로 '아동 대상 서비스로 취급'을 요청할 수 있도록 허용해야 합니다. 이러한 취급은 미국 아동 온라인 개인 정보 보호법(COPPA) 및 EU 개인 정보 보호법(GDPR) 을 포함한 관련 법률 및 규정을 준수하여 이루어져야 합니다.
  - Google Play는 '아동 대상 서비스로 취급'의 일환으로 광고 SDK에서 개인 맞춤 광고, 관심 기반 광고, 리마케팅을 사용 중지하도록 요구합니다.
- 아동을 대상으로 광고를 게재하기 위해 실시간 입찰을 사용하는 경우 개인 정보 보호 표시가 입찰자에게 전달되도록 해야 합니다.
- 아동 또는 연령 미상인 사용자의 AAID, SIM 일련번호, 빌드 일련번호, BSSID, MAC, SSID, IMEI 및/또는 IMSI를 전송해서는 안 됩니다.

5. **미디에이션 플랫폼:** 아동을 대상으로 광고를 게재하는 경우 다음을 준수해야 합니다.
   - 가족용 자체 인증 광고 SDK만 사용하거나 미디에이션에서 게재된 모든 광고가 이러한 요건을 준수하도록 필요한 보호 장치를 구현합니다.
   - 광고 콘텐츠 등급 및 해당하는 '아동 대상 서비스로 취급'을 표시하는 데 필요한 정보를 미디에이션 플랫폼에 전달합니다.
6. **자체 인증 및 규정 준수:** 광고 SDK 정책이 다음을 포함하되 이에 국한되지 않는 모든 자체 인증 요건을 준수하는지 확인할 수 있도록 충분한 정보(예: 신청 양식 에 명시된 정보)를 Google에 제공해야 합니다.
   - SDK 또는 미디에이션 플랫폼의 서비스 약관, 개인정보처리방침, 게시자 통합 가이드를 영문 버전으로 제공해야 합니다.
   - 규정을 준수하는 최신 버전의 광고 SDK를 사용하는 샘플 테스트 앱 제출. 샘플 테스트 앱은 완전하게 빌드되어 실행 가능하며 SDK의 모든 기능을 활용하는 Android APK여야 합니다. 테스트 앱 요건은 다음과 같습니다.
     - 휴대전화 폼 팩터에서 실행되도록 설계되었으며 완전히 빌드되고 실행 가능한 Android APK로 제출되어야 합니다.
     - Google Play 정책을 준수하는 최신 버전 또는 곧 출시될 버전의 광고 SDK를 사용해야 합니다.
     - 광고 SDK를 호출하여 광고를 검색하고 표시하는 등 광고 SDK의 모든 기능을 사용해야 합니다.
     - 현재 광고 게재에 사용 중인 네트워크의 모든 광고 인벤토리를 테스트 앱에서 요청된 광고 소재를 통해 완전히 사용할 수 있어야 합니다.
     - 지리적 위치에 따라 제한되어서는 안 됩니다.
     - 인벤토리가 여러 연령대를 대상으로 하는 경우 테스트 앱은 전체 인벤토리의 광고 소재 요청과 아동 또는 모든 연령대에 적합한 인벤토리의 광고 소재 요청을 구분할 수 있어야 합니다.
     - 중립적인 연령 심사에 의해 제어되는 경우가 아니라면 테스트 앱은 인벤토리 내의 특정 광고로 제한되어서는 안 됩니다.
7. 개발자는 후속 정보 요청에 시의적절하게 응답하고 출시되는 모든 신규 버전이 가족 정책 요건을 비롯한 최신 Google Play 개발자 프로그램 정책을 준수한다는 것을 자체적으로 인증 해야 합니다.
8. **법률 준수:** 가족용 자체 인증 광고 SDK는 게시자에게 적용될 수 있는 아동 관련 법령과 규정을 모두 준수하는 광고 게재 서비스를 지원해야 합니다.
   - SDK 또는 미디에이션 플랫폼이 미국 아동 온라인 개인 정보 보호법(COPPA) , EU 개인 정보 보호법(GDPR) 및 기타 관련법 또는 규정을 준수하도록 해야 합니다.

     참고: '아동'이라는 단어는 언어와 상황에 따라 서로 다른 대상을 의미할 수 있습니다. 변호사의 도움을 받아 앱에 적용될 수 있는 의무사항 또는 연령에 따른 제한사항을 확인해야 합니다. 앱이 어떻게 작동하는지는 개발자가 가장 잘 알고 있으므로 Google은 개발자가 제공한 정보를 바탕으로 Google Play에서 공개되는 앱이 가족에게 안전하다는 것을 확인합니다.

프로그램 요건에 관한 자세한 내용은 가족용 자체 인증 광고 SDK 프로그램 페이지를 참고하세요.

시정 조치

정책을 위반한 다음에 상황을 관리하는 것보다는 정책 위반이 되지 않도록 주의하는 편이 훨씬 낫습니다. 하지만 Google에서는 위반 사례가 발생했을 때 개발자에게 어떻게 하면 정책을 잘 지키는 앱을 만들 수 있는지 알려 드리기 위해 노력합니다. 위반 사례를 발견 하거나 위반 사항 관리 에 관해 궁금한 점이 있으면 알려주세요.

정책 적용 범위

Google의 콘텐츠 정책은 개발자의 앱이 사용자에게 표시하는 광고, 앱이 호스팅하거나 링크를 제공하는 사용자 제작 콘텐츠와 같이 앱이 표시하거나 링크를 제공하는 모든 콘텐츠에 적용됩니다. 또한 개발자 이름과 등록된 개발자 웹사이트의 방문 페이지를 포함하여 Google Play에 공개적으로 표시되는 개발자 계정의 모든 콘텐츠에도 적용됩니다.

사용자가 다른 앱을 기기에 설치할 수 있게 하는 앱은 허용되지 않습니다. 제3자가 제공하는 기능 및 환경을 포함하여 다른 앱, 게임 또는 소프트웨어에 설치 없이 액세스하는 기능을 제공하는 앱의 경우 액세스 권한을 제공하는 모든 대상 콘텐츠가 Google Play 정책을 모두 준수해야 하며, 추가 정책 검토의 대상이 될 수도 있습니다.

이 정책에서 사용된 정의 용어는 개발자 배포 계약(DDA)에서와 같은 의미를 가집니다. 이러한 정책 및 DDA를 준수하는 것 외에도 앱의 콘텐츠는 Google의 콘텐츠 등급 가이드라인에 따라 등급이 지정되어야 합니다.

Google Play 생태계에서 사용자의 신뢰를 훼손하는 앱 또는 앱 콘텐츠는 허용되지 않습니다. Google Play에서 앱을 포함할지 또는 삭제할지 결정할 때, Google은 유해한 동작 패턴이나 높은 악용 위험성을 포함하되 이에 국한되지 않는 다양한 요소를 고려합니다. Google에서는 특정 앱 및 개발자를 대상으로 한 불만사항, 뉴스 보도, 이전 위반 내역, 사용자 의견 및 인기 브랜드, 캐릭터, 기타 저작물 사용을 포함하되 이에 국한되지 않는 다양한 항목을 통해 악용될 위험성을 파악합니다.

Google Play 프로텍트의 원리

Google Play 프로텍트는 사용자가 설치하는 앱을 검사하며, 주기적으로 기기도 검사합니다. 잠재적으로 위험한 앱이 감지되면 다음과 같이 처리합니다.

- 알림을 전송합니다. 앱을 삭제하려면 알림을 탭한 후 제거를 탭합니다.
- 앱을 제거할 때까지 앱을 사용 중지합니다.
- 앱을 자동으로 삭제합니다. 대부분의 경우 유해 앱이 감지되어 삭제되었다는 알림이 표시됩니다.

멀웨어 차단 기능의 원리

악의적인 타사 소프트웨어, URL 및 기타 보안 문제로부터 사용자를 보호하기 위해 Google은 다음에 관한 정보를 수신할 수 있습니다.

- 기기의 네트워크 연결
- 잠재적으로 위험한 URL
- 운영체제, 그리고 Google Play 또는 다른 소스를 통해 기기에 설치된 앱

안전하지 않을 수 있는 앱이나 URL에 관한 Google의 경고가 표시되는 경우도 있습니다. 기기, 데이터, 사용자에게 유해한 것으로 알려진 앱 또는 URL의 경우 Google이 기기에서 삭제하거나 설치를 차단할 수 있습니다.

이러한 보호 기능 중 일부는 사용자가 기기 설정에서 사용 중지할 수 있습니다. 하지만 Google은 Google Play를 통해 설치된 앱에 관한 정보를 계속 수신할 수 있으며, 다른 소스를 통해 기기에 설치된 앱은 보안상의 이유로 계속 검사될 수 있으나 Google에 정보가 전달되지는 않습니다.

개인정보 보호 알림 작동 방식

Google Play 프로텍트는 앱이 사용자의 개인 정보에 액세스할 수 있다는 문제로 Google Play 스토어에서 삭제된 경우 알림을 표시합니다. 이때 앱을 제거할 수 있는 옵션도 표시됩니다.

시정 조치 절차

콘텐츠 또는 계정을 검토하여 불법 또는 정책 위반 여부를 판단할 때는 앱 메타데이터(예: 앱 제목 및 설명), 인앱 환경, 계정 정보(예: 과거 정책 위반 내역), 앱 내 모든 서드 파티 코드, 보고 메커니즘(해당하는 경우) 및 자체 이니셔티브 검토를 통해 제공된 기타 정보 등 다양한 정보를 고려하여 결정을 내립니다. 앱에서 사용되는 모든 서드 파티 코

드(예: SDK) 및 앱과 관련된 해당 서드 파티의 관행이 모든 Google Play 개발자 프로그램 정책을 준수하는지 확인해야 할 책임은 개발자에게 있습니다.

앱 또는 개발자 계정이 Google 정책을 위반할 경우 Google은 아래와 같이 적절한 조치를 취합니다. 또한 조치가 잘못되었다고 판단할 경우의 이의신청 방법에 관한 안내와 함께 Google이 취한 조치의 관련 정보를 이메일로 제공해 드립니다.

삭제 또는 관리 알림이 계정, 앱 또는 앱 카탈로그에 있는 모든 정책 위반 사례를 언급하는 것은 아니라는 점을 유의하시기 바랍니다. 개발자는 모든 정책 문제에 대응하고 추가로 상당한 주의를 기울여 앱 또는 계정의 나머지 부분이 완전히 정책을 준수하도록 해야 할 의무가 있습니다. 계정 및 모든 앱의 정책 위반 문제를 해결하지 못할 경우 추가 시정 조치로 이어질 수 있습니다.

이러한 정책 또는 개발자 배포 계약 (DDA)의 반복적이거나 심각한 위반(예: 멀웨어, 사기, 사용자나 기기에 해를 끼칠 수 있는 앱)으로 인해 개인 또는 관련 Google Play 개발자 계정이 해지될 수 있습니다.

시정 조치

각각의 시정 조치는 여러 가지 방식으로 앱에 영향을 미칠 수 있습니다. Google 정책을 위반하여 사용자와 Google Play 생태계 전반에 유해한 영향을 미치는 콘텐츠를 감지하고 평가하기 위해 Google에서는 직접 평가 방식과 자동 평가 방식을 함께 활용하여 앱과 앱 콘텐츠를 검토합니다. 자동화된 모델을 사용하면 더 많은 위반 사례를 감지하고 잠재적인 문제를 더 빠르게 평가할 수 있으며, 이는 모두에게 안전한 Google Play 환경을 제공하는 데 도움이 됩니다. 정책을 위반하는 콘텐츠는 자동화된 모델에 의해 삭제되거나, 콘텐츠 일부의 맥락을 이해해야 하는 경우와 같이 더 정밀한 판단이 필요한 경우 훈련을 받고 평가를 수행하는 운영자와 분석가가 추가로 검토할 수 있도록 신고됩니다. 이러한 직접 검토의 결과는 이후 머신러닝 모델 개선을 위한 학습 데이터를 구축하는 데 사용됩니다.

다음 섹션에서는 Google Play에서 취할 수 있는 다양한 조치와 앱 및/또는 Google Play 개발자 계정에 미치는 영향을 설명합니다.

시정 조치 커뮤니케이션에서 달리 명시하지 않는 한 이러한 조치는 모든 지역에 적용됩니다. 예를 들어 앱이 정지될 경우 모든 지역에서 사용할 수 없게 됩니다. 또한 개발자가 조치에 대해 이의신청을 제출하고 이의신청이 승인되지 않는다면 달리 명시되지 않는 한 해당 조치는 그 효력을 유지합니다.

거부

- 검토를 위해 제출된 신규 앱 또는 앱 업데이트는 Google Play에서 사용할 수 있는 상태가 아닙니다.
- 기존 앱의 업데이트가 거부된 경우 이 업데이트 이전에 게시된 앱 버전은 Google Play에서 계속 제공됩니다.
- 거부하더라도 거부한 앱의 기존 사용자 설치 수, 통계, 평점에 관한 액세스 권한에는 영향을 미치지 않습니다.
- 거부하더라도 Google Play 개발자 계정의 상태에는 영향을 미치지 않습니다.

참고: 정책 위반사항을 모두 수정하기 전까지는 거부된 앱을 다시 제출하지 마시기 바랍니다.

삭제

- 앱은 모든 이전 버전과 함께 Google Play에서 삭제되며 사용자가 더 이상 다운로드할 수 없게 됩니다.
- 앱이 삭제되기 때문에 사용자는 앱의 스토어 등록정보를 확인할 수 없습니다. 삭제된 앱을 정책에 맞게 업데이트하여 제출하면 이 정보는 복원됩니다.
- 정책을 준수하는 버전이 Google Play에서 승인되기 전까지는 사용자가 인앱 구매를 하거나 인앱 결제 기능을 사용할 수 없습니다.
- 삭제가 Google Play 개발자 계정의 상태에 즉시 영향을 주지는 않지만, 앱이 여러 번 삭제되면 정지될 수 있습니다.

참고: 정책 위반사항을 모두 수정하기 전까지는 삭제된 앱을 다시 제출하지 마시기 바랍니다.

계정 정지

- 앱은 모든 이전 버전과 함께 Google Play에서 삭제되며 사용자가 더 이상 다운로드할 수 없게 됩니다.
- 반복하여 또는 심각한 수준으로 정책을 위반할 경우, 그리고 앱이 여러 번 거절되거나 삭제되는 경우 정지될 수 있습니다.

- 앱이 정지되기 때문에 사용자는 앱의 스토어 등록정보를 확인할 수 없습니다.
- 정지된 앱의 APK 또는 App Bundle은 더 이상 사용할 수 없습니다.
- 사용자가 인앱 구매를 하거나 앱의 인앱 결제 기능을 사용할 수 없습니다.
- 정지는 경고로 간주되므로 Google Play 개발자 계정의 양호한 상태에 부정적인 영향을 미칩니다. 경고를 여러 번 받으면 개인 계정과 관련 Google Play 개발자 계정이 해지될 수 있습니다.

제한된 공개 상태

- Google Play에서 앱의 검색 가능 여부가 제한됩니다. 앱은 Google Play에서 계속 제공되며 앱의 스토어 등록정보로 직접 연결되는 링크를 통해 사용자가 액세스할 수도 있습니다.
- 앱을 제한된 공개 상태로 설정해도 Google Play 개발자 계정의 상태에는 영향을 미치지 않습니다.
- 앱을 제한된 공개 상태로 설정해도 사용자가 앱의 기존 스토어 등록정보를 보는 데 영향을 주지 않습니다.

제한된 지역

- 사용자가 특정 지역에서만 Google Play를 통해 앱을 다운로드할 수 있습니다.
- 다른 지역의 사용자는 Play 스토어에서 앱을 찾을 수 없습니다.
- 이전에 앱을 설치한 사용자는 계속해서 기기에서 앱을 사용할 수 있으나 더 이상 업데이트는 받을 수 없습니다.
- 지역 제한이 Google Play 개발자 계정의 상태에 영향을 주지는 않습니다.

계정이 제한된 상태

- 개발자 계정이 제한된 상태가 되면 카탈로그의 모든 앱이 Google Play에서 삭제되며 더 이상 새로운 앱을 게시하거나 기존 앱을 다시 게시할 수 없게 됩니다. Play Console에는 계속 액세스할 수 있습니다.
- 모든 앱이 삭제되기 때문에 사용자는 앱의 스토어 등록정보와 개발자 프로필을 확인할 수 없습니다.
- 현재 사용자가 인앱 구매를 하거나 앱의 인앱 결제 기능을 사용할 수 없습니다.
- 계속해서 Play Console을 사용하여 Google Play에 추가 정보를 제공하고 계정 정보를 수정할 수 있습니다.
- 모든 정책 위반을 수정한 후 앱을 다시 게시할 수 있습니다.

계정 해지

- 개발자 계정이 해지되면 카탈로그의 모든 앱이 Google Play에서 삭제되며 더 이상 새로운 앱을 게시할 수 없게 됩니다. 또한 관련 Google Play 개발자 계정도 영구적으로 정지됩니다.
- 여러 번 정지되거나 심각한 정책 위반으로 정지되는 경우 Play Console 계정이 해지될 수도 있습니다.
- 해지된 계정에 포함된 앱이 삭제되기 때문에 사용자는 앱의 스토어 등록정보와 개발자 프로필을 확인할 수 없습니다.
- 현재 사용자가 인앱 구매를 하거나 앱의 인앱 결제 기능을 사용할 수 없습니다.

참고: 새로운 계정을 개설하려고 시도하면 이러한 계정 역시 개발자 등록 수수료의 환불 없이 해지되므로 다른 계정이 해지된 상태에서는 새로운 Play Console 계정을 등록하지 마시기 바랍니다.

휴면 계정

휴면 계정이란 비활성 상태이거나 한동안 사용되지 않은 개발자 계정입니다. 휴면 계정은 개발자 배포 계약 에서 요구되는 양호한 상태에 해당하지 않습니다.

Google Play 개발자 계정은 앱을 게시하고 적극적으로 유지 관리하는 활성 상태의 개발자를 위한 계정입니다. Google Play에서는 악용을 막기 위해 휴면 상태이거나 사용하지 않는 계정을 해지하고 있습니다. 앱 게시 및 업데이트, 통계 액세스, 스토어 등록정보 관리 등의 정기적 활동이 현저히 적은 계정도 마찬가지입니다.

휴면 계정 해지는 사용자의 계정이 해지됨을 의미합니다. 휴면 계정을 복구하지 않으면 Google Play Console 내의 모든 보고서, 통계, 인사이트 또는 기타 정보를 더 이상 사용할 수 없게 됩니다. 등록 수수료는 환불되지 않고 소멸됩니다. Google Play에서는 휴면 계정을 해지하기 전에 개발자가 제공한 계정 연락처 정보를 통해 계정 해지를 알립니다.

휴면 계정이 해지되더라도 향후 아무런 제약 없이 Google Play에 앱을 게시하기 위한 새로운 계정을 만들 수 있습니다.

정책 위반 관리 및 신고

시정 조치에 관한 이의 제기

오류로 인해 조치가 적용된 것이고, 애플리케이션이 Google Play 프로그램 정책 및 개발자 배포 계약을 위반하지 않는다고 판단되는 경우 애플리케이션을 복구해 드립니다. 정책을 신중하게 검토한 후 Google의 결정이 잘못되었다고 생각되면 시정 조치 이메일 알림에 제공된 안내에 따르거나 여기를 클릭하여 결정에 이의신청하시기 바랍니다.

추가 리소스

시정 조치 또는 사용자의 평점/댓글에 관한 추가 정보가 필요한 경우 아래 리소스를 참고하거나 Google Play 고객센터를 통해 문의할 수 있습니다. Google에서는 법률 자문을 제공할 수 없으니 법률 자문이 필요한 경우 변호사와 상담하시기 바랍니다.

- 앱 인증
- 정책 위반 신고
- 계정 해지 또는 앱 삭제와 관련해 Google Play에 문의하기
- 합당한 경고
- 부적절한 앱 및 댓글 신고
- 앱이 Google Play에서 삭제됨
- Google Play 개발자 계정 해지에 관해 알아보기

Play Console 요구사항

활발한 앱 생태계의 안전과 보안을 위해 Google Play는 모든 개발자로 하여금 프로필을 Play Console 개발자 계정에 연결하는 등 Play Console 요구사항을 충족하도록 요구하고 있습니다. 사용자가 개발자에게 신뢰와 확신을 가질 수 있도록 Google Play에는 인증된 정보가 표시됩니다. Google Play에 표시되는 정보에 관해 자세히 알아보세요.

Google Play에서는 두 가지 개발자 계정 유형(개인 및 조직)이 제공됩니다. 올바른 개발자 계정 유형을 선택하고 필요한 인증을 완료하는 것이 원활한 온보딩 환경의 핵심입니다. 개발자 계정 유형 선택에 관해 자세히 알아보세요.

Play Console 계정을 만들 때 다음 서비스를 제공하는 개발자는 조직으로 등록해야 합니다.

- 금융 상품 및 서비스(은행, 대출, 주식 거래, 투자 펀드, 암호화폐 소프트웨어 지갑, 암호화폐 거래소를 포함하되 이에 국한되지 않음). 금융 서비스 정책에 관해 자세히 알아보세요.
- 건강 앱(예: 의료 앱 및 인간 대상 연구 앱). 건강 앱 카테고리에 관해 자세히 알아보세요.
- VpnService 클래스를 사용하도록 승인된 앱. VPN 서비스 정책에 관해 자세히 알아보세요.
- 정부 앱(정부 기관에서 또는 정부 기관을 대신하여 개발한 앱 포함)

계정 유형을 선택한 후에는 다음 사항을 준수해야 합니다.

- 다음 세부정보를 포함하여 개발자 계정 정보를 정확하게 제출합니다.
  - 법적 이름 및 주소
  - D-U-N-S 번호 (조직으로 등록하는 경우)
  - 담당자 이메일 주소 및 전화번호
  - Google Play에 표시할 개발자 이메일 주소 및 전화번호(해당하는 경우)
  - 결제 수단(해당하는 경우)
  - 개발자 계정에 연결된 Google 결제 프로필

- 조직으로 등록하는 경우 개발자 계정 정보가 최신 상태이며 Dun & Bradstreet 프로필에 저장된 세부정보와 일치해야 합니다.

앱을 제출하기 전에는 다음 사항을 준수해야 합니다.

- 모든 앱 정보와 메타데이터를 정확하게 입력합니다.
- 앱의 개인정보처리방침을 업로드하고 데이터 보안 섹션 요구사항을 작성합니다.
- 활성 상태의 데모 계정, 로그인 정보는 물론 Google Play에서 앱을 검토하는 데 필요한 기타 모든 리소스(구체적으로 로그인 사용자 인증 정보, QR 코드 등)를 제공합니다.

언제나 그렇듯이 앱은 안정적이고 몰입감 있으며 반응이 빠른 사용자 환경을 제공해야 합니다. 광고 네트워크, 분석 서비스, 서드 파티 SDK 등 앱의 모든 요소가 Google Play 개발자 프로그램 정책을 준수하는지 다시 한번 확인하세요. 앱 타겟층에 아동이 포함되어 있는 경우에는 가족 정책을 준수해야 합니다.

개발자 배포 계약 및 모든 개발자 프로그램 정책을 검토하여 앱이 정책을 준수하도록 할 책임은 개발자에게 있습니다.

Developer Distribution Agreement

도움이 더 필요하신가요?

다음 단계를 시도해 보세요.

도움말 커뮤니티에 게시하기
커뮤니티 회원의 답변 받기

문의하기
자세히 알려주시면 도움을 드리겠습니다.