开发者计划政策

（将于 2025 年 8 月 27 日起生效，除非另有说明）

让我们一起打造全球最值得信赖的应用和游戏平台

您的创新推动我们共同迈向成功，但取得成就的同时也伴随着责任。这些开发者计划政策和开发者分发协议可以确保我们一起携手通过 Google Play 不断向超过 10 亿的用户提供全球最具创新性和最值得信赖的应用。欢迎您详细了解我们的下列各项政策。

受限内容

每天都有世界各地的用户从 Google Play 下载应用和游戏。在提交应用之前，请先仔细想想，您的应用是否适合在 Google Play 发布以及是否符合当地法律规定。

危害儿童

如果应用不禁止用户创建、上传或分发煽动剥削或虐待儿童的内容，我们会立即将其从 Google Play 下架。这包括所有儿童性虐待内容。如要举报 Google 产品中将儿童作为剥削对象的内容，请点击**举报滥用行为**。如果您在互联网上的其他地方发现此类内容，请直接与您所在国家/地区的相关机构联系。

我们禁止使用任何会危害儿童的应用。这包括但不限于使用应用宣传针对儿童的掠夺性行为，例如：

- 针对儿童的不当互动（例如抚摸或爱抚）。
- 诱骗儿童（例如，在网上结交儿童以达到与该儿童在线上或线下进行性接触以及/或者与其交换色情照片的目的）。
- 将未成年人性欲化（例如，描绘、鼓动或宣扬对儿童进行性虐待的图像，或是以可能导致儿童遭到性剥削的方式描绘儿童的内容）。
- 性勒索（例如，通过真实或声称拥有的儿童私密照来威胁或勒索儿童）。
- 拐卖儿童（例如，为达到商业性剥削目的而宣传或引诱儿童）。

一旦发现应用中包含儿童性虐待内容，我们便会采取相应措施，其中可能包括向美国全国失踪与受虐儿童服务中心 (NCMEC) 举报。如果您认为某名儿童面临危险或遭到虐待、剥削或拐卖，请与您当地的执法机构联系，并联系此处所列的某个儿童安全组织。

此外，我们也不允许面向儿童的应用中出现成人主题，包括但不限于：

- 含有过度暴力和血腥的内容。
- 描绘或鼓励有害、危险的活动。

我们也不允许应用宣传负面身体形象或自我形象，包括出于娱乐目的描绘整形手术、减肥以及对个人外表进行的其他美容调整。

“儿童安全标准”政策

Google Play 要求社交应用和约会交友应用遵循我们的“儿童安全标准”政策。

这类应用必须：

- **具有已发布的标准：**您的应用必须在可公开访问的标准（例如应用服务条款、社区准则或任何其他公开提供的用户政策文档）中明确禁止儿童性虐待和性剥削 (CSAE) 行为。
- **提供应用内用户反馈机制：**您必须以自行认证的形式证明，您在应用内提供了相应机制，使用户能够在应用内提交反馈、反映疑虑或报告问题。
- **处理儿童性虐待内容 (CSAM)：**您必须以自行认证的形式证明，根据您发布的标准和相关法律，您的应用在确切获知其中存在儿童性虐待内容后会采取适当措施，包括但不限于移除相应内容。

- **遵守《儿童安全法》：**您必须以自行认证的形式证明，您的应用遵守适用的儿童安全法律法规，包括但不限于设有专门的流程，可将已确认的儿童性虐待内容报告给美国全国失踪与受虐儿童援助中心 或您所在地区的相关机构。
- **提供儿童安全事宜联系人：**您的应用必须提供一名指定的联系人，负责接收 Google Play 可能就您的应用或平台中发现的儿童性虐待和性剥削内容发送的通知。这名代表必须能够说明您的违规处置和审核程序相关事宜，并在必要时采取相应措施。

如需详细了解这些要求以及如何遵守要求，请参阅我们的帮助中心文章。

不当内容

为确保 Google Play 始终是一个安全文明的平台，我们制定了一套标准来定义对用户有害或不当的内容，并禁止此类内容出现在我们的平台上。

色情内容和亵渎性内容

我们禁止任何应用包含或宣传色情内容或粗言秽语，包括淫秽内容或以性取悦为目的的任何内容或服务。我们禁止任何疑似宣传或招揽有偿性行为的应用或应用内容。我们禁止任何应用包含或宣传与性掠夺行为相关的内容，或在未经当事人同意的情况下散布色情内容。如果裸露内容主要用作教育、纪实、科学或艺术用途，确实有纳入或宣传的必要，则不在此限。

目录应用（即在内容目录中列出图书/视频作品的应用）可以发布包含色情内容的图书（包括电子书和有声读物）或视频作品，但需要符合以下要求：

- 包含色情内容的图书/视频作品仅占该应用总体目录的一小部分
- 应用不会主动宣传包含色情内容的图书/视频作品。这些作品仍可根据用户历史记录显示在推荐中，或者在一般价格促销活动期间显示。
- 应用不会分发任何包含危害儿童的内容、淫秽内容或适用法律认定违法的任何其他色情内容的图书/视频作品
- 应用通过限制未成年人访问包含色情内容的图书/视频作品来保护未成年人

如果应用包含违反此政策的内容，但这些内容在某个特定地区被认为是适当的内容，则应用可以面向该地区的用户提供，但不允许面向其他地区的用户提供。

下面是常见违规行为的一些示例：

- 描绘色情性裸体或性挑逗姿势的内容，其中所描绘的主体为裸体、经过模糊处理、衣着极度暴露和/或衣着不适合公共场合。
- 包含对性行为或性挑逗姿势的描绘、动画或插图，或包含对身体部位的色情性描绘。
- 描绘性辅助用品、性爱指南、非法性爱主题和恋物癖的内容，或具有此类功能的内容。
- 包含淫秽或粗言秽语，包括但不限于商品详情或应用中含脏话、下流语言、露骨文字或成人/色情关键字的内容。
- 描绘、描述或鼓动人兽性交的内容。
- 应用宣传了性爱相关娱乐活动、陪侍服务或其他可能会被解读为提供或招揽有偿性行为的服务，包括但不限于有偿约会或色情交易，在这类服务中约会的一方依预期或暗示要向另一方提供金钱、礼品或经济支持（“包养约会”）。
- 贬低或物化他人，例如宣称能脱去人的衣服或透过衣服看到身体，即使标明是恶作剧或娱乐性质的应用，也同样在禁止之列。
- 试图以性方式威胁或剥削他人的内容或行为，例如偷拍、隐藏摄像头、通过深度伪造或类似技术制作的非自愿性内容，或侵犯内容。

仇恨言论

我们不允许任何应用基于种族或族群、宗教信仰、残障、年龄、国籍、退伍军人身份、性取向、性别、性别认同、种姓、移民身份或者与制度性歧视/边缘化相关的其他特征，针对个人或群体宣扬暴力或煽动仇恨。

在某些国家/地区，根据当地的法律法规，如果应用包含与纳粹相关的 EDSA（教育、纪实、科学或艺术）内容，也可能会被屏蔽。

下面是常见违规行为的一些示例：

- 包含声称受保护群体毫无人性、低人一等或应该被仇视的内容或言论。
- 包含仇恨辱骂、成见或受保护群体具有负面特质（例如恶毒、堕落、邪恶等）的观点，或明示/暗示该群体是一种威胁。
- 包含试图鼓动他人相信受保护群体应受到仇视或歧视的内容或言论。
- 包含宣扬与仇恨团体相关的标志、符号、徽章、用品或行为等仇恨象征的内容。

暴力内容

我们不允许发布描绘或助长无端暴力或其他危险活动的应用。通常情况下，如果应用描绘的是卡通、打猎或钓鱼等游戏性虚构暴力内容，则在允许发布之列。

下面是常见违规行为的一些示例：

- 以图形或文字形式描绘对任何人或动物的写实暴力行为或暴力威胁。
- 宣传自残、自杀、进食障碍、窒息游戏或其他可能导致严重伤亡的行为。

暴力极端主义

我们禁止恐怖组织以任何目的（包括招募人员）在 Google Play 上发布应用。其他参与、准备针对平民的暴力行动，或声称对此类行动负责的危险组织或运动亦在禁止之列。

我们不允许应用包含与暴力极端主义有关的内容，也不允许应用包含与策划、准备或美化针对平民的暴力行动有关的内容，例如宣扬恐怖行动、煽动暴力或庆祝恐怖袭击的内容。如果是出于教育、纪实、科学或艺术目的发布有关暴力极端主义的内容，请务必提供相关的 EDSA 背景信息。

敏感事件

我们不允许任何应用利用具有重大的社会、文化或政治影响的敏感事件（例如民事紧急事件、自然灾害、公共卫生紧急事件、冲突、死亡或其他悲剧事件），也不接受对这些事件缺乏敏感性的应用。如果应用包含的敏感事件相关内容具有教育、纪实、科学研究或艺术 (EDSA) 价值或旨在提醒用户关注敏感事件或提高认知度，则通常在允许发布之列。

下面是常见违规行为的一些示例：

- 对于因自杀、药物过量、自然原因等导致的实际人员或群体死亡缺乏敏感性。
- 否认发生过有据可查的重大悲剧事件。
- 涉嫌利用敏感事件牟利，且不会给受害者带来任何明显利益。

欺凌和骚扰

我们不允许任何应用包含威胁、骚扰或欺凌性内容，或助长威胁、骚扰或欺凌行为。

下面是常见违规行为的一些示例：

- 欺凌国际冲突或宗教冲突的受害者。
- 内容涉及意图剥削他人，包括勒索、敲诈等。
- 为了公开羞辱某人而发布内容。
- 骚扰悲剧事件的受害者或其亲朋好友。

危险品

我们不允许任何应用为炸药、枪支、弹药或特定枪支配件的销售提供便利，

- 管制配件包括可将枪支改造成仿自动或全自动枪支的配件（如撞火枪托、加特林扳机、自动退壳阻铁、改装工具包）以及可容纳超过 30 发子弹的弹匣或弹链。

我们不允许应用提供制造炸药、枪支、弹药、管制枪支配件或其他武器的操作说明，包括将枪支改造成全自动或仿自动射击武器的说明。

大麻

我们不允许任何应用为大麻或大麻制品的销售提供便利，无论这种行为是否合法。

下面是常见违规行为的一些示例：

- 允许用户通过应用内购物车功能订购大麻。
- 协助用户安排大麻的运送或取货事宜。
- 为销售包含 THC（四氢大麻酚）的产品提供便利，包括含有 THC 的 CBD 油等产品。

烟草制品和酒精饮料

我们不允许任何应用为销售烟草或含尼古丁的产品（如电子烟和尼古丁袋）提供便利，或鼓吹非法或不当饮酒、吸烟或吸食尼古丁的行为。

其他信息

- 禁止描绘或鼓动未成年人抽烟喝酒或向未成年人贩卖烟酒。
- 禁止暗示抽烟可提高社交能力、性功能、专业能力、知识水平或运动能力。
- 禁止以肯定的态度描述过量饮酒行为，包括以积极正面的口吻描述过量饮酒、狂饮或拼酒的场面。
- 禁止以烟草产品为主题发布广告、开展宣传或进行精选展示（其中包括广告、横幅、类别以及指向烟草销售网站的链接）。
- 在某些地区，我们可能会允许食品/日杂配送应用在遵守相关限制的前提下销售烟草产品，但须具备年龄限制保护措施（例如，在送货时查验身份）。
- 我们可能会允许销售作为戒烟辅助工具来宣传的产品，前提是产品具备年龄限制保护措施。

金融服务

我们不允许 Google Play 中的任何应用向用户提供或宣传具有欺骗性或危害性的金融产品和服务。

在本政策中，“金融产品和服务”是指与资金和加密货币的管理或投资相关的产品和服务，包括个性化理财建议。

如果您的应用提供或宣传金融产品和服务，则必须遵守应用所面向的目标国家/地区的国家和地方法规。例如，应用中必须包含当地法律要求提供的特定披露信息。

无论任何应用，只要包含金融功能，都必须在 Play 管理中心内填写“金融功能声明表单”。

二元期权

我们不允许任何应用向用户提供二元期权交易功能。

贷款

个人贷款：我们所定义的个人贷款是指由个人、组织或实体向消费者个人提供的一次性贷款，且款项并非用于购买固定资产或支付教育费用。您应向有意申请个人贷款的消费者提供与贷款产品的质量、特点、费用、还款计划、风险和权益有关的信息，帮助消费者就是否贷款做出明智决定。

- 示例：个人贷款、发薪日贷款、P2P 网络贷款、所有权贷款
- 不属于个人贷款的示例：抵押贷款、汽车贷款、循环信用贷款（例如信用卡、个人信用贷款）

工资随取：我们所定义的工资随取 (EWA) 贷款是一种金融服务，可让个人支取一部分已赚取但雇主尚未支付的工资。与传统贷款不同，EWA 服务具有以下特征：

- 还款机制：通过扣除工资或与用户银行账户关联的自动还款交易来自动还款。即使自动还款交易失败，也不会收取额外的利息、罚款或费用。
- 按收入支取：用户可支取的金额不能超过其在当前支付期内已经赚取的工资，从而确保用户不会透支未来的收入。
- 费用结构：EWA 服务不收取利息，而是会收取较低的固定费用或按百分比计算的交易费用作为服务费。合理的费用应尽可能低且公开透明，足以反映提供此类服务的实际成本，但又不会给用户增加负担，每笔交易的费用可能在 1 至 5 美元或预支金额的 1-5% 之间。
- 不会形成债务：EWA 服务通常不会向信用机构报告此类交易，以确保相应交易不会影响用户的信用评分，也不会导致长期债务累积。

提供个人贷款的应用（包括但不限于直接提供此类贷款的应用、贷款推广应用，以及为消费者与第三方贷款机构牵线搭桥的贷款中介应用）必须在 Play 管理中心内将应用类别设置为“财务”，并在应用元数据中披露以下信息：

- 最短还款期和最长还款期。
- 最高年利率 (APR)：通常包括一年的利率加上服务费及其他费用，或依据当地法律计算的其他类似费率。
- 贷款总费用的代表性示例，其中应包括本金以及所有适用费用。
- 隐私权政策，其中应全面披露对用户个人数据和敏感用户数据进行的访问、收集、使用和分享行为（该政策受本政策中列出的限制条件的约束）。

我们不允许应用推广要求在贷款发放之日起 60 天或更短时间内全额还款的个人贷款（我们称之为“短期个人贷款”）。

提供工资随取贷款的应用（包括但不限于直接提供此类贷款的应用、贷款推广应用，以及为消费者与第三方贷款机构牵线搭桥的贷款中介应用）必须在 Play 管理中心内将应用类别设置为“金融”，并在应用元数据中披露以下信息：

- 还款条款及条件。
- 所有费用，包括订阅费用、交易费用以及与提供贷款相关的所有其他费用。
- 贷款总费用的代表性示例，其中应包括所有费用。
- 隐私权政策，其中应全面披露对用户个人数据和敏感用户数据进行的访问、收集、使用和分享行为（该政策受本政策中列出的限制条件的约束）。

我们必须能够确认您的开发者账号与所提供的许可或文件之间的关联，以证明您具备提供个人贷款服务的资质。我们可能需要您提供额外信息或文件，以确认您的账号符合所有当地法律法规。

我们禁止以下应用获取照片和通讯录之类的敏感数据：个人贷款应用；以促成个人贷款为主要用途的应用（例如贷款推广应用或贷款中介应用）；信用额度方面的应用、贷款附属应用或信用方面的应用（贷款计算器、贷款指导类应用等）；工资随取 (EWA) 应用。禁止获取以下权限：

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

利用敏感信息或敏感 API 的应用必须遵循额外的限制和要求。如需了解更多信息，请参阅权限政策。

高年利率个人贷款

在美国，我们不允许应用提供或宣传年利率 (APR) 达到或超过 36% 的个人贷款。在美国，个人贷款应用必须展示其贷款的最高年利率，且年利率的计算方法必须遵守《诚信贷款法案》(TILA)　。

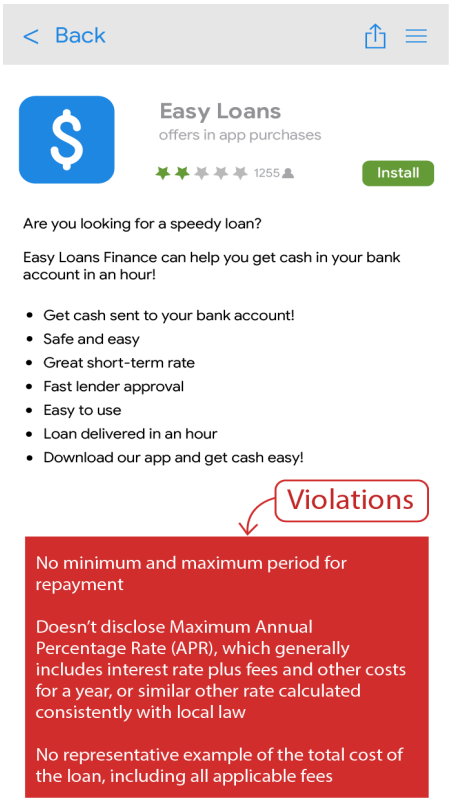
本政策适用于直接提供贷款的应用、贷款推广应用以及为消费者与第三方贷款机构牵线搭桥的贷款中介应用。

针对具体国家/地区的要求

以所列国家/地区境内用户为目标受众群体的个人贷款应用必须遵守额外的要求，并在 Play 管理中心内的金融产品和服务声明中提供补充证明文件。提供工资随取 (EWA) 贷款的应用须遵守这些要求，前提是这些要求在相关管辖区内适用。此外，您还必须根据 Google Play 的要求提供其他相关信息或文件，以证明您遵守适用的法规和许可要求。

1. **印度**
   - 如果您已获得印度储备银行 (RBI) 的许可，可以提供个人贷款，则必须提交许可副本供我们审核。
   - 如果您不直接参与借贷活动，只是提供一个平台，方便已注册的非银行金融公司 (NBFC) 或银行向用户放款，您需要在声明中准确说明这一点。
     - 此外，请务必在应用说明中醒目地披露所有已注册的 NBFC 和银行的名称。
2. **印度尼西亚**
   - 如果您的应用根据印尼金融服务监管局颁布的第 77/POJK.01/2016 号法令（可能会不时修订），参与基于信息技术的金钱借贷服务，则您必须提交有效许可的副本供我们审核。
3. **菲律宾**
   - 凡是通过在线借贷平台 (OLP) 提供贷款的金融和放款公司，都必须从菲律宾证券交易委员会 (PSEC) 取得 SEC 注册编号和授权证书 (CA) 编号。
     - 此外，请务必在应用说明中披露您的公司名称、商家名称、PSEC 注册编号，以及授权您经营金融/放款公司的授权证书 (CA)。
   - 如果应用参与基于借贷的众筹活动（例如 P2P 网络借贷），或是参与与众筹相关的法规和规章（CF 规定）所定义的活动，则必须通过已在 PSEC 注册的众筹中介机构来处理交易。
4. **尼日利亚**
   - 数字贷款机构 (DML) 必须遵循尼日利亚联邦竞争与消费者保护委员会 (FCCPC) 颁布的《2022 年数字贷款有限临时监管/注册框架和指南》（可能会不时修订）并填写相关表单，还必须获得由 FCCPC 提供的可验证的批准函。
   - 贷款服务聚合商必须提供数字借贷服务的文件和/或证明，以及每个合作 DML 的详细联系信息。
5. **肯尼亚**
   - 数字分期付款提供商 (DCP) 应完成 DCP 注册流程，并获得肯尼亚中央银行 (CBK) 颁发的许可。您必须在声明中提供 CBK 所颁发许可的副本。
   - 如果您不直接参与借贷活动，只是提供一个平台，方便已注册的 DCP 向用户放款，您需要在声明中准确说明这一点，并提供相应合作伙伴的 DCP 许可副本。
   - 目前，我们仅接受 CBK 官方网站的“数字分期付款提供商名录”下公示的实体所提供的声明和许可。
6. **巴基斯坦**
   - 每个非银行金融机构 (NBFC) 贷方只能发布一款数字贷款应用 (DLA)。如果开发者试图针对每个 NBFC 发布多款 DLA，则可能导致开发者账号和任何其他关联账号被终止。
   - 您必须提交巴基斯坦证券交易委员会 (SECP) 签发的批准证明，才能在巴基斯坦提供或协助用户获得数字贷款服务。另外，禁止发布短期贷款应用；不过，如果巴基斯坦的法律法规明确准许，可能会有极少数例外情况。
7. **泰国**
   - 如果个人贷款应用以泰国境内用户为目标受众群体，且贷款利率不低于 15%，则必须获得泰国银行 (BoT) 或泰国财政部 (MoF) 颁发的有效许可。开发者必须提供相关文件，证明其有能力在泰国提供个人贷款或为此类服务提供便利。此类文件应包括：
     - 泰国银行颁发的个人贷款提供商或纳米金融（小额贷款）组织经营许可的副本。
     - 泰国财务部颁发的 Pico 或 Pico-plus 贷款机构 Pico-Finance 牌照的副本。

下面是常见违规行为的示例：



现金赌博、游戏和竞赛

我们允许发布符合特定要求的现金赌博应用、与现金赌博相关的广告、游戏化的会员回馈活动以及每日梦幻运动游戏应用。

赌博应用

我们允许在遵守相关限制和所有 Google Play 政策的情况下，在指定的国家/地区发布让用户能在线赌博或为在线赌博提供便利的应用，但前提如下：应用的开发者必须为通过 Google Play 分发的赌博应用完成申请流程 ，其资质为经批准的政府性运营机构，并且/或者是已在指定国家/地区的相应赌博主管部门登记的许可运营机构，同时还要提供在指定国家/地区推出相应类型在线赌博产品所需的有效运营许可证。

我们仅允许发布提供以下类型在线赌博产品且获得有效许可或授权的赌博应用：

- 在线赌场游戏
- 体育博彩
- 赛马（在监管和许可方面独立于体育博彩）
- 彩票
- 每日梦幻运动游戏

符合条件的应用必须满足以下要求：

- 开发者必须已成功完成申请流程，可以在 Google Play 上分发应用；
- 应用必须遵守每个分发国家/地区的所有适用法律和业界标准；
- 开发者必须具备应用所分发到的每个国家/地区或州/区域的有效赌博许可；
- 开发者不得提供超出其赌博许可范围的赌博产品；
- 应用必须防止未满规定年龄的用户使用；
- 应用必须防止开发者提供的赌博许可未涵盖的国家/地区、州或地理区域的用户进行访问和使用；
- 应用不得以付费应用的形式在 Google Play 上架供用户购买，也不得使用 Google Play 应用内购买结算功能；
- 应用必须可供用户从 Google Play 商店免费下载和安装；

- 应用的分级必须为 AO（仅限成人）或 IARC 的同等分级；并且
- 应用及其应用详情必须清楚显示有关理性赌博的信息。

其他现金游戏、竞赛和比赛应用

对于所有不符合上述赌博应用资格要求且下述“其他现金游戏测试”未涵盖的其他应用，我们不允许其中包含的任何内容或服务让用户可以进行以下活动或为此类活动提供便利：使用现金（包括用现金购买的应用内商品）下注、押注或参与活动，以赢取具有真实货币价值的奖励。这包括但不限于接受付费且提供现金或其他现实有价物奖励的在线赌场、体育博彩、彩票和游戏（符合下文“游戏化的会员回馈活动”部分所述要求的活动除外）。

违规行为示例

- 游戏让玩家可以通过付费来换取赢得实物奖励或现金奖励的机会
- 应用提供含有相关“号召性用语”的导航元素或功能（例如菜单项、标签页、按钮、WebView 等），让用户使用现金下注、押注或参与现金游戏、竞赛或比赛，例如应用会在比赛中邀请用户“马上下注！”“马上注册！”或“马上参加！”，让用户有机会赢取现金奖励。
- 应用接受或管理押注、应用内代币、奖金或押金，从而让用户能参与有实物或货币奖励的赌博或获得此类奖励。

其他现金游戏（测试）

我们有时会在特定地区针对某些类型的现金游戏开展限时测试。如需了解详情，请参阅此帮助中心页面。在日本开展的在线夹娃娃游戏测试于 2023 年 7 月 11 日结束。从 2023 年 7 月 12 日开始，在遵守适用法律并满足特定要求的情况下，在线夹娃娃游戏应用可在全球各地的 Google Play 上架。

游戏化的会员回馈活动

在法律允许且不受其他赌博或游戏许可要求限制的情况下，我们允许开展以实物或等价现金奖励用户的会员回馈活动，但此类活动必须符合以下 Play 商店资格要求：

针对所有应用（游戏类　和非游戏类）：

- 会员回馈活动的福利或奖励必须明确附属于且从属于应用内符合条件的相应付费交易（符合条件的付费交易必须是真正的独立交易，以提供与会员回馈活动无关的商品或服务为目的），并且福利或奖励不能通过购买而获得，也不得与违反“现金赌博、游戏和竞赛”政策限制规定的任何其他形式的交易相关联。
  - 例如，符合条件的付费交易中不得有任何为参与会员回馈活动而支付的费用或赌注，并且符合条件的付费交易不得因给予用户福利或奖励而致使商品或服务的购买价格高于正常价格。

针对游戏类　应用：

- 如果积分或奖励的福利或奖品与符合条件的付费交易相关联，那么用户只能按固定比率赢取和兑换相应的积分或奖励，比率必须在应用中以及公开发布的官方活动规则内醒目地载明；福利或可兑换价值的赢取**不得**以用户的游戏表现或凭运气得到的结果为胜负依据、奖励依据或指数计算依据。

针对非游戏类应用：

- 在满足下述要求的情况下，积分或奖励可以与竞赛或凭运气得到的结果相关联。如果会员回馈活动的福利或奖励与符合条件的付费交易相关联，那么活动必须满足以下要求：
  - 在应用内发布活动的官方规则。
  - 如果活动采用灵活奖励、凭运气得奖或具有随机性的奖励机制：活动的官方条款中必须披露 1) 在按固定获奖几率确定奖励的会员回馈活动中，获奖几率是多少，以及 2) 在所有其他此类会员回馈活动中，采用何种选择获奖者的方法（例如用以确定奖励的变量因素）。
  - 如果活动提供抽奖、抓彩或其他类似形式的促销奖励，官方条款中必须说明每项促销奖励的固定获奖人数、固定的参与截止时间和发奖日期。
  - 如果积分或会员回馈活动奖励要按固定比率累积和兑换，则应用中和活动的官方条款内必须醒目地载明比率。

提供会员回馈活动的应用类型	会员回馈活动游戏化，奖励灵活变化	会员回馈奖励按固定比率/时间安排提供	必须有会员回馈活动条款及条件	对于凭运气得奖的会员回馈活动，其条款及条件中必须披露获奖几率或选择获奖者的方法
游戏类应用	不允许	允许	强制要求	不适用（游戏类应用的会员回馈活动不得含有凭运气得奖的元素）
非游戏类应用	允许	允许	强制要求	强制要求

在通过 Play 分发的应用中投放赌博广告或现金游戏、竞赛和比赛的广告

只有在满足下列要求的前提下，我们才允许应用投放宣传赌博、现金游戏、竞赛和竞标赛的广告：

- 应用和广告（包括广告主）必须遵守广告投放地区的所有适用法律和业界标准；
- 广告必须符合当地对于宣传任何赌博相关产品和服务的所有适用广告许可要求；
- 应用不得向已知未满 18 周岁的用户展示赌博广告；
- 应用不得加入亲子同乐计划；
- 应用不得将未满 18 周岁的用户作为目标受众群体；
- 如果要宣传赌博应用（如上文所定义），广告必须在着陆页、所宣传的应用详情本身或应用内清楚显示有关理性赌博的信息；
- 应用不得提供模拟赌博内容（例如社交类赌场应用、具有虚拟老虎机的应用）；
- 应用不得提供赌博或现金游戏、彩票或锦标赛的辅助/配套功能（例如，协助进行下注、付款、体育赛事比分/赔率/赛绩跟踪或管理参赛金的功能）；
- 应用内容不得宣传或引导用户使用赌博或现金游戏、彩票或赛事服务

只有符合上文所列部分中所有这些要求的应用才能包含宣传赌博或现金游戏、彩票或锦标赛的广告。获得许可的赌博应用（如上文所定义）或符合上方 1-6 条要求且获得许可的每日梦幻运动游戏应用（如下文所定义）可包含宣传赌博或现金游戏、彩票或锦标赛的广告。

违规行为示例

- 某款应用专为未成年用户设计，但却展示宣传赌博服务的广告
- 某款模拟赌场游戏宣传或引导用户前往现金赌场
- 某款专门跟踪体育赛事赔率的应用包含链接至体育博彩网站的赌博广告
- 应用包含违反欺骗性广告政策的赌博广告，例如以按钮、图标或其他互动式应用内元素的形式向用户展示广告

每日梦幻运动游戏 (DFS) 应用

只有在满足以下要求的前提下，我们才允许发布适用的当地法律所定义的每日梦幻运动游戏 (DFS) 应用：

- 应用 1) 仅在美国分发，或者 2) 符合上述适用于美国以外国家/地区的“赌博应用”相关要求和申请流程的规定；
- 开发者必须成功完成 DFS 申请　流程并获得许可，才能在 Play 上分发应用；
- 应用必须遵守各个分发国家/地区的所有适用法律和业界标准；
- 应用必须防止未满规定年龄的用户在应用中押注或进行货币交易；
- 应用不得以付费应用的形式在 Google Play 上架供用户购买，也不得使用 Google Play 应用内购买结算功能；
- 应用必须可供用户从 Play 商店免费下载和安装；
- 应用的分级必须为 AO（仅限成人）或 IARC 的同等分级；
- 应用及其应用详情必须清楚显示有关理性赌博的信息；
- 如果应用面向美国的某些州或地区分发，则必须遵守相应州或地区的所有适用法律和业界标准；
- 美国某些州或地区规定每日梦幻运动游戏应用开发者必须拥有相关许可，因此开发者必须在相应地区取得有效许可；

- 如果开发者在美国某些州或地区尚未获得每日梦幻运动游戏应用所需的许可，则必须防止这些州或地区的用户使用该应用；并且
- 在美国某些州或地区，每日梦幻运动游戏应用不合法，开发者必须防止这些州或地区的用户使用此类应用。

非法活动

我们不允许发布宣传或助长非法活动的应用。

下面是常见违规行为的一些示例：

- 为买卖违禁药品提供便利。
- 描绘或鼓动未成年人使用或贩卖非法药品、酒精饮料或烟草。
- 提供有关如何种植或制造违禁药品的说明。

用户生成的内容

用户生成的内容 (UGC) 是指用户向应用提交的内容，至少有一部分应用用户可以看到或访问此类内容。

包含或主打 UGC 的应用（包括将用户导向 UGC 平台的特殊浏览器或客户端）必须持续实施完善有效的 UGC 审核机制：

- 在用户创建或上传 UGC 前，要求用户接受应用的使用条款和/或用户政策；
- 根据 Google Play 开发者计划政策定义不良内容和行为，并在应用的使用条款或用户政策中禁止此类内容和行为；
- 针对应用包含的 UGC 的类型，以合理一致的方式实施 UGC 审核管理机制。这包括提供应用内系统，用于屏蔽和举报令人反感的 UGC 与用户，以及在适当的情况下针对此类 UGC 和/或用户采取相应措施。不同的 UGC 体验可能需要不同的管理审核措施。例如：
  - 如果应用主打 UGC，并通过用户验证或离线注册等方式识别指定的用户组（例如，专用于特定学校或公司等组织的应用），则必须提供用于举报内容/用户的应用内功能。
  - 如果 UGC 功能支持特定用户之间进行一对一互动（例如，私信、标记、提及等），则必须提供用于屏蔽用户的应用内功能。
  - 如果应用提供对可供公开访问的 UGC 的访问权限（例如社交应用和博主应用），则必须实现用于举报用户/内容以及屏蔽用户的应用内功能。
  - 在增强现实 (AR) 应用中，UGC 审核机制（包括应用内举报系统）必须同时考虑以下因素：不良的 AR UGC（例如露骨色情 AR 图片）和敏感的 AR 锚定位置（例如 AR 内容锚定至军事基地等受限区域，或锚定至 AR 锚定可能会给地产所有者带来问题的私人地产）。
- 采取防护措施，以防用户通过鼓动令人反感的用户行为在应用内变现。

附随性色情内容

如果出现色情内容的 UGC 应用 (1) 主要是提供非色情内容；(2) 不会主动宣传或推荐色情内容，相关色情内容则属于“附随性”色情内容。若按照适用法律规定，色情内容为违法或危害儿童的内容，则不属于“附随性”色情内容，且一律受到禁止。

符合下列所有要求的 UGC 应用可以包含附随性色情内容：

- 这类内容默认被过滤器隐藏，而用户至少需要执行两项操作才能完全停用这类过滤器（例如隐藏在混淆处理的插页后方，或是未停用“安全搜索”就默认不会显示在视图上）。
- 利用年龄筛查系统（例如无倾向年龄筛查机制或适用法律规定的适当系统），明确禁止儿童访问该应用（有关儿童的定义，请参见家庭政策）。
- 开发者根据内容分级政策的规定，在应用的内容分级调查问卷中如实回答与 UGC 相关的问题。

如果应用的主要用途是提供不良 UGC，Google Play 会将其下架。同样地，如果应用的主要用途最终演变为存放不良 UGC，或因含有大量此类内容而在用户群体中广为人知，Google Play 也会将其下架。

下面是常见违规行为的一些示例：

- 宣传露骨色情 UGC，包括实现或允许主要用于鼓动分享令人反感的内容的付费功能。
- 应用包含 UGC，但未针对威胁、骚扰或欺凌性内容（尤其是面向未成年人的此类内容）采取充分的保护措施。
- 应用中发布的帖子、评论或照片主要目的在于骚扰他人或专门辱骂、恶意攻击或嘲笑某个人。
- 应用含有令人反感的内容，用户投诉颇多但一直未得到解决。

健康内容和服务

我们不允许任何应用向用户提供危害健康的内容和服务。

如果您的应用包含或宣传健康类内容和服务，则必须遵守所有适用的法律法规。

健康类应用

如果您的应用会访问健康数据，而且属于健康类应用或具有健康相关功能，则该应用不仅必须遵守现有的 Google Play 开发者政策（包括“隐私权、欺骗行为和滥用”政策和“敏感事件”政策），还必须满足以下要求：

- **管理中心声明：**
  - 前往 Play 管理中心的“应用内容”页面（“政策”>“应用内容”），然后选择应用所属的一个或多个类别。
- **隐私权政策和关于提供醒目披露声明的要求：**
  - 您的应用必须在 Play 管理中心内的指定字段中发布隐私权政策链接，并在应用内发布隐私权政策链接或文本。请确保您的隐私权政策能够通过可公开访问且未设定地理围栏的有效网址（而非 PDF）查看，且不可编辑（根据“数据安全”部分的要求）。
  - 应用的隐私权政策（以及任何形式的应用内披露声明）必须详尽地说明您的应用访问、收集、使用及分享个人数据或敏感用户数据的方式，不限于上文所述“数据安全”部分中披露的数据。对于受危险权限或运行时权限 管制的任何功能或数据，应用必须满足所有适用的关于提供醒目披露声明和征求用户同意的要求。
  - 不得请求健康类应用执行其核心功能时并不需要的权限，而且必须移除用不到的权限。如需查看被视为涉及健康相关敏感数据的权限列表，请参阅健康类应用及其他信息。
  - 如果应用本质上不是健康类应用，但提供健康相关功能并会访问健康数据，则仍须满足“健康类应用”政策的相关要求。此类应用应该向用户明确说明应用的核心功能与收集健康相关数据的行为之间的关联（例如，保险提供商、通过收集用户的活动数据来推动游戏情节发展的游戏应用等）。应用的隐私权政策必须体现这一使用限制。
- **其他要求：**
  如果您的健康类应用属于以下类别之一，您必须遵守相关要求，并且在 Play 管理中心内选择相应的类别：
  - **与政府有关联的健康应用：**如果您获得了政府或公认的医疗保健机构的许可，可以开发并分发与他们存在关联的应用，您必须通过提前通知表单提交资格证明。
  - **接触者追踪/健康状况应用：**如果您的应用是接触者追踪和/或健康状况应用，请在 Play 管理中心内选择“疾病预防和公共健康”，然后通过上文所述的提前通知表单提供所需的信息。
  - **人体研究应用：**开展与健康相关的人体研究的应用必须遵守所有适用规则和法规，包括但不限于征得参与者本人或（如果参与者是未成年人）其父母/监护人的知情同意。除非另有豁免，否则健康研究应用还应获得机构审查委员会 (IRB) 和/或同等独立伦理委员会的批准。在提出请求时，必须提供此类批准的证明。
  - **医疗设备或 SaMD 应用：**被视为医疗设备或医疗设备独立软件 (SaMD) 的应用必须获得并持有由负责该健康应用的管理及法规遵从的监管部门或机构提供的许可证或其他批准文件。在提出请求时，必须提供此类许可证或批准的证明。

Health Connect 数据

通过 Health Connect 权限访问的数据属于个人数据及敏感的用户数据，对这些数据的使用必须遵循用户数据 政策以及其他要求 。

处方药

我们不允许任何应用为在未经医生开立处方的情况下买卖处方药提供便利。

未获批准的药物成分

Google Play 不允许应用宣传或销售未获批准的药物成分，即使声称合法，也不例外。

下面是常见违规行为的一些示例：

- 这份违禁药物和补充剂 清单（非详尽清单）中的所有产品。
- 含有麻黄成分的产品。
- 涉及用人体绒毛膜促性腺激素 (hCG) 减肥/控制体重的产品，或与合成类固醇放在一起宣传的产品。
- 含有活性药物成分或危险成分的草本和膳食补充剂。
- 虚假或误导性健康声明，包括在声明中暗示该产品的效果等同处方药或管制药物。
- 未经政府审批的产品，但在宣传时暗示可安全或有效地预防、治愈或治疗某种疾病或病症。
- 政府或监管机构的行动或警告中涉及的产品。
- 产品所用名称与未获批准的药品/补充剂或管制药物相似，可能会造成混淆。

如需详细了解我们监控的未获批准或具有误导性的药品和补充剂，请访问 www.legitscript.com 。

有关健康的虚假信息

我们不允许任何应用包含与现有医学共识相悖或可能会对用户造成伤害的误导性健康声明。

下面是常见违规行为的一些示例：

- 关于疫苗的误导性声明，例如疫苗会改变一个人的 DNA。
- 宣扬有害且未经批准的治疗方法。
- 宣扬其他有害健康的做法，例如转化疗法。

医疗功能

我们不允许任何应用提供具有误导性或潜在危害的医疗或健康相关功能。例如，应用不得声称可完全依靠应用本身提供血氧测量功能。血氧计应用需要额外硬件支持才能提供血氧测量功能，相关硬件可能为：外部硬件、穿戴式设备或智能手机内专为支持血氧测量功能设计的传感器。这些有硬件支持的应用也必须在元数据内包含免责声明，声明本身并非供医疗使用，也不是医疗设备，仅适用于一般的健身/健康用途，并以适当的方式披露兼容的硬件型号/设备型号。

付款 - 临床服务

涉及受监管的临床服务的交易不应使用 Google Play 结算系统。如需了解详情，请参阅了解 Google Play 付款政策 。

基于区块链的内容

随着区块链技术持续快速发展，我们力求为开发者提供一个平台，使其能够通过创新实现蓬勃发展并为用户打造更丰富的沉浸式体验。

在本政策中，“基于区块链的内容”是指在区块链上受到保护的代币化数字资产。如果您的应用包含基于区块链的内容，您必须遵守这些要求。

加密货币交易所和软件钱包

加密货币的购买、持有或兑换应通过受监管管辖区内经认证的服务机构进行。

此外，您还必须遵守应用的所有目标国家/地区的适用法规，并避免在您的产品和服务被禁的国家/地区内发布您的应用。Google Play 可能会要求您提供其他相关的信息或文件，以证明您遵守所有适用的法规要求或

许可要求。

挖矿

我们不允许任何应用在设备上进行加密货币挖矿，但允许应用远程管理加密货币的挖矿操作。

针对分发代币化数字资产的透明度要求

如果您的应用销售代币化数字资产，或使用户能够赚取此类资产，您必须通过 Play 管理中心“应用内容”页面上的“金融功能”声明表单声明此情况。

创建应用内商品时，您必须在商品详情中指明其代表了一种代币化数字资产。如需获得更多指导信息，请参阅创建应用内商品。

您不得宣传或美化可能通过玩游戏或交易活动赚取的任何收益。

针对 NFT 游戏化机制的附加要求

根据 Google Play“现金赌博、游戏和竞赛”政策的要求，集成了代币化数字资产（例如 NFT）的赌博应用应该完成相应申请流程。

对于所有不符合赌博应用资格要求且其他现金游戏（测试）未涵盖的其他应用，不应接受任何具有货币价值的物品来换取获得价值不明的 NFT 的机会。用户购买的 NFT 应该在游戏中消费或使用，以增强用户体验或帮助用户推进游戏进程。NFT 不得用于进行下注或抵押，以换取赢得具有真实货币价值的奖品（包括其他 NFT）的机会。

下面是常见违规行为的一些示例：

- 应用出售 NFT 套装，但未披露 NFT 的具体内容和价值。
- 付费制社交博弈类游戏（例如老虎机）提供 NFT 做为奖励。

AI 生成的内容

生成式 AI 模型是一项可供越来越多的开发者使用的技术，您也可能会将此类模型整合到您的应用中，以提高互动度并改进用户体验。Google Play 希望协助您确保 AI 生成的内容对所有用户而言都是安全的，并整合用户反馈，推动实现负责任的创新。

AI 生成的内容

AI 生成的内容是指由生成式 AI 模型根据用户提示生成的内容。AI 生成的内容的示例包括：

- 支持文字到文字对话的生成式 AI 聊天机器人，这类应用的核心功能是与聊天机器人互动
- 由 AI 根据文字、图片或语音提示生成的图片或视频

为确保用户的安全并符合 Google Play 的政策覆盖范围，如果应用使用 AI 生成内容，则必须符合现有的 Google Play 开发者政策，包括禁止和防止生成受限内容，例如煽动剥削或虐待儿童的内容，以及促成欺骗性行为的内容。

如需了解生成式 AI 应用内容安全防护的业界最佳实践的资源，请参阅我们的这篇帮助中心文章。

如果应用使用 AI 生成内容，则必须包含应用内用户举报或标记功能，让用户无需退出应用即可向开发者举报或标记冒犯性内容。开发者应以用户举报的信息作为完善应用内容过滤和管理机制的依据。

知识产权

我们既不允许任何应用或开发者帐号侵犯他人的知识产权（包括商标、版权、专利、商业机密和其他专有权利），也不允许任何应用鼓动或诱使他人侵犯知识产权。

只要我们收到有关涉嫌侵犯版权的明确通知，就会作出回应。如需了解更多信息或根据《数字千年版权法案》(DMCA) 提交请求，请参阅我们的版权规程 。

如需针对在应用内销售或促销仿冒商品的行为提交投诉，请提交仿冒投诉 。

如果您是商标所有人，并且认为 Google Play 上的某款应用侵犯了您的商标权，建议您直接与开发者联系以解决问题。如果您无法与开发者达成解决方案，请通过此表单 提交商标投诉。

如果您有书面文件可证明您有权在自己的应用或商品详情中使用第三方知识产权内容（例如品牌名称、徽标和图片资产），请在提交您的应用之前与 Google Play 团队联系 ，以确保您的应用不会因侵犯知识产权而被拒绝。

在未经授权的情况下使用受版权保护的内容

我们不允许任何应用侵犯版权。即使开发者对受版权保护的内容进行了修改，仍可能会导致违规行为。如需使用受版权保护的内容，开发者可能需要提供相关权利证明。

在使用受版权保护的内容来展示应用的功能时，请务必谨慎。一般来说，最安全的做法就是打造原创内容。

下面是常见违规行为的一些示例：

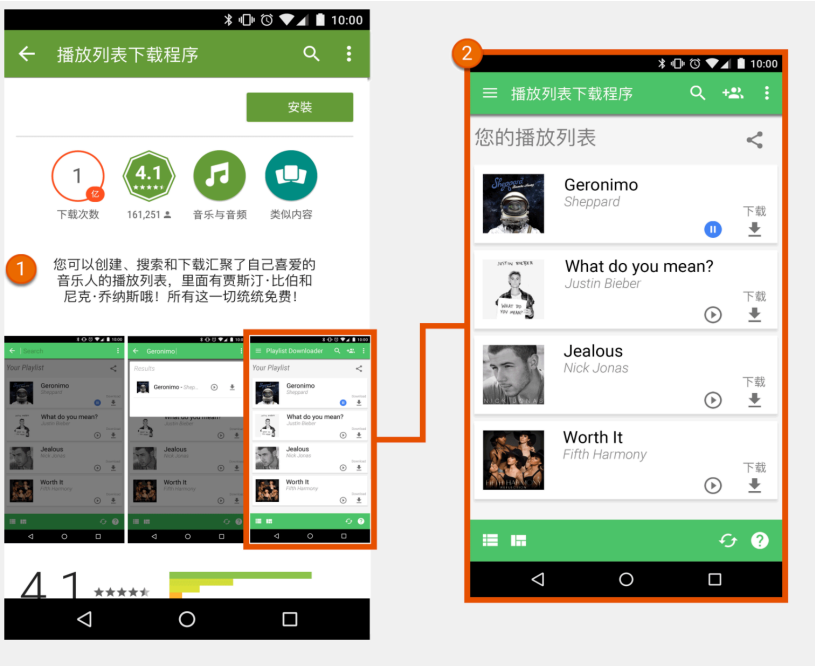
- 音乐专辑、视频游戏和图书的封面/封底图片。
- 电影、电视或视频游戏的营销图片。
- 漫画、卡通、电影、音乐视频或电视的海报图片或图片。
- 大学校队和专业运动队的徽标。
- 从公众人物的社交媒体帐号中提取的照片。
- 公众人物的专业形象。
- 与受版权保护的原创作品高度相似的复制品或同人作品。
- 应用包含来自受版权保护内容的音频剪辑的音效集。
- 非公共领域图书的完整复制版或翻译版。

鼓动他人侵犯版权

我们不允许任何应用诱使或鼓动他人侵犯版权。在发布应用之前，请先检查您的应用是否可能以任何方式鼓动他人侵犯版权，并在必要时进行法律咨询。

下面是常见违规行为的一些示例：

- 允许用户在未经授权的情况下将受版权保护的内容下载到本地的影音在线播放应用。
- 鼓动用户在违反适用版权法的情况下在线播放和下载受版权保护的作品（包括音乐和视频）的应用：



① 此应用商品详情中的说明鼓动用户在未经授权的情况下，下载受版权保护的内容。
② 此应用商品详情中的屏幕截图鼓动用户在未经授权的情况下，下载受版权保护的内容。

商标侵权

我们不允许任何应用侵犯他人商标权。商标是标识商品或服务来源的字词、符号或两者的组合。商标一经获得，即意味着其所有者享有将该商标用于特定商品或服务的专有权力。

商标侵权是指以不当方式或在未经授权的情况下使用相同或相似商标，可能导致对相关商品的来源造成混淆。如果您的应用以可能造成混淆的方式使用第三方的商标，那么我们可能会暂停您的应用。

仿冒

我们禁止任何应用销售或促销仿冒商品。仿冒商品使用与其他商品完全相同或高度相似的商标或徽标，从而模仿正品的品牌特征，以期达到鱼目混珠的效果。

隐私权、欺骗行为和设备滥用

我们致力于保护用户隐私，为用户提供安全可靠的环境。对于具有欺骗性或恶意性质的应用，以及试图滥用或不当使用任何网络、设备或个人数据的应用，我们一律严格禁止。

用户数据

您必须清楚说明您会如何处理用户数据（例如从用户那里收集到的信息或与用户相关的信息，包括设备信息）。也就是说，您必须披露应用访问、收集、使用、处理及分享用户数据的方式，并且仅将这些数据用于已披露的合规用途。请注意，在处理用户个人数据和敏感用户数据时，还必须同时遵守以下“用户个人数据和敏感用户数据”部分的其他要求。除了这项和其他 Play 开发者计划政策之外，您还必须始终遵守您提供的产品/服务所在管辖区内适用的隐私及数据保护法。例如，如果您向欧盟境内用户提供服务，请注意，法国数据保护机构 (CNIL) 采用了移动环境内个人数据保护最佳实践指南 ，值得您多加参考。

如果您的应用中包含第三方代码（例如 SDK），那么您必须确保应用中使用的第三方代码，以及相应第三方对应用中用户数据的处理做法，均符合 Google Play 开发者计划政策，包括使用要求和信息披露要求。例如，您必须确保 SDK 提供方不会出售应用中的用户个人数据和敏感用户数据。无论用户数据是在发送到服务器后进行传输，还是通过在应用中嵌入第三方代码进行传输，此要求都适用。

个人数据和敏感用户数据

个人数据和敏感用户数据包括但不限于个人身份信息、财务和付款信息、身份验证信息、电话簿、通讯录、设备位置信息 、短信和通话相关数据、健康数据 、Health Connect 数据、设备上其他应用的清单、麦克风数据、摄像头数据，以及其他敏感的设备或使用情况数据。如果您的应用将会处理个人数据和敏感用户数据，您必须满足以下要求：

- 只有在出于提供应用和服务功能，以及用户合理预期的符合政策要求的目的时，才可以访问、收集、使用和分享通过应用获取的个人数据和敏感用户数据：
  - 如果应用还将个人数据和敏感用户数据用于广告的投放，则必须遵守 Google Play 广告政策 。
  - 此外，如果您需要将相关数据传输给服务提供商 ，或因合法理由（例如遵守有效的政府要求、依据适用法律的规定，或作为合并或收购的一部分）需要传输相关数据，则在依法向用户做出适当通知的前提下，可以进行传输。
- 以安全的方式处理所有个人数据和敏感用户数据，包括使用新型加密技术（例如通过 HTTPS）传输数据。
- 在访问受 Android 权限 控制的数据之前，应尽可能使用运行时权限请求。
- 不出售个人数据和敏感用户数据。
  - “出售”是指以换取金钱为目的，将个人数据和敏感用户数据交换或传输给第三方 。
    - 用户发起的个人数据和敏感用户数据传输行为（例如，当用户使用应用的某项功能将文件传输给第三方时，或当用户选择使用专用的调研应用时）不视为出售。

关于提供醒目披露声明与征求用户同意的要求

如果您的应用对个人数据和敏感用户数据的访问、收集、使用或分享方式不在相关产品或功能的用户的合理预期范围内（例如，如果数据收集行为发生在后台，即用户未与应用进行互动时），您必须满足以下要求：

醒目披露声明：您必须提供应用内披露声明，说明您对数据的访问、收集、使用和分享行为。应用内披露声明必须满足以下所有要求：

- 必须在应用内明示，不得只在应用说明或网站中显示；
- 必须在用户正常使用应用的情况下显示，并且无需用户打开任何菜单或设置就能查看；
- 必须说明要访问或收集的数据类型；
- 必须说明数据的使用和/或分享方式；
- 不得只列在隐私权政策或服务条款中；
- 不得包含在其他与个人数据和敏感用户数据收集无关的披露声明中。

应用内用户意见征求和运行时权限请求：这些请求之前必须紧接符合本政策要求的应用内披露声明。在征求用户同意时，必须满足以下所有要求：

- 意见征求对话框必须以清楚明确的方式呈现；
- 必须要求用户执行明确的确认操作（例如点按接受、勾选复选框）；
- 不得将用户离开披露声明页面的操作（包括点按其他位置离开或按下返回或主屏幕按钮）视为同意；
- 不得使用会自动关闭或设有期限的消息作为征得用户同意的方式；并且
- 必须在用户授予权限后，您的应用才能开始收集或访问个人数据和敏感用户数据。

如果应用因其他法律依据需在未征得用户同意的情况下处理个人数据和敏感用户数据（例如欧盟《一般数据保护条例》[GDPR] 规定的合法权益），则必须遵守所有适用的法律要求，并向用户提供适当的披露，包括本政策要求的应用内披露。

为了符合政策要求，建议您在必要时参考以下醒目披露声明的示例格式：

- “[此应用]会收集/传输/同步处理/存储[数据类型]，以便[在使用情境下]支持[‘功能’]。”
- *示例：“为支持‘健身跟踪’功能，Fitness Funds 会收集位置信息数据，即使应用处于关闭或未使用状态，也仍会收集这些数据；此外，这些数据还会用于支持广告投放。”*
- *示例：“Call Buddy 会收集、读取和写入通话记录数据以支持联系人整理功能，甚至在未使用应用的情况下也会执行这些操作。”*

如果您的应用集成了旨在默认收集个人数据和敏感用户数据的第三方代码（例如 SDK），您必须在收到 Google Play 请求后的 2 周内（或者，如果 Google Play 的请求提供了更长的期限，则以相应期限为准）提供足够的证据，以证明您的应用符合本政策中关于提供醒目披露声明和征求用户同意的要求，包括关于通过第三方代码访问、收集、使用或分享数据的要求。

下面是常见违规行为的一些示例：

- 应用会收集设备位置信息，但未提供醒目披露声明，说明哪些功能会使用这类数据及/或指明应用在后台的使用情形。
- 应用在未提供指明数据用途的醒目披露声明的情况下，就已经具备请求访问数据的运行时权限。
- 应用会获取用户已安装应用的目录信息，但并未将此类数据视为受上述隐私权政策、数据处理要求，以及醒目披露声明和征求用户同意相关要求所保护的个人数据或敏感数据。
- 应用会获取用户的电话或通讯录数据，但并未将此类数据视为受上述隐私权政策、数据处理要求，以及醒目披露声明和征求用户同意相关要求所保护的个人数据或敏感数据。
- 应用会记录用户的屏幕画面，但未将此类数据视为受这项政策保护的个人数据或敏感数据。
- 应用会收集设备位置信息 ，但未按照上述要求全面披露其使用情况并征得用户同意。
- 应用出于跟踪、研究或营销等目的，在后台使用受限权限，但未按照上述要求全面披露其使用情况并征得用户同意。
- 应用使用 SDK 收集个人数据和敏感用户数据，但未按照本用户数据政策的要求、数据访问/处理（包括禁止的出售行为）方面的要求，以及关于提供醒目披露声明和征求用户同意的要求来处理这些数据。

如需详细了解关于提供醒目披露声明和征求用户同意的要求，请参阅这篇文章。

对访问个人数据及敏感数据的限制

除了上述要求之外，下表还介绍了针对具体活动的要求。

活动	要求
您的应用会处理财务信息、付款信息或政府提供的身份证件号	应用不得公开披露与财务、付款活动或者政府提供的身份证件号相关的任何个人数据及敏感的用户数据。
您的应用会处理非公开的电话簿或联系信息	我们禁止在未经授权的情况下擅自发布或披露他人的非公开联系信息。
您的应用包含防病毒或安全防护功能，如防病毒、反恶意软件或相关安全防护功能	您的应用必须提供隐私权政策，在此政策以及任何形式的应用内披露声明中，须说明您的应用要收集和传输哪些用户数据、如何使用这些数据以及数据分享对象的类型。
您的应用的目标用户是儿童	您的应用不得包含未获准用于面向儿童的服务的 SDK。请参阅设计适合儿童和家庭的应用 ，了解所有政策内容及要求。
您的应用会收集或关联永久性设备标识符（例如IMEI、IMSI、SIM 卡序列号等）	请勿将永久性设备标识符与其他个人数据、敏感的用户数据或可重置的设备标识符相关联，以下用途除外： • 用于与 SIM 身份信息关联的电话服务（例如关联到某个运营商帐号的 Wi-Fi 通话服务）； • 用于以设备所有者模式运行的企业设备管理应用。 必须按照用户数据政策 中的规定向用户醒目地披露此类用途。 如需了解其他唯一标识符，请参阅此资源 。 如需了解 Android 广告 ID 方面的其他指南，请参阅广告政策 。

“数据安全”部分

所有开发者都必须在每个应用中提供清晰准确的“数据安全”部分，详细说明用户数据的收集、使用和分享方式。开发者应负责确保标签的准确性并及时更新相关信息。如适用，“数据安全”部分应与应用的隐私权政策中披露的信息一致。

如需详细了解如何完成“数据安全”部分，请参阅这篇文章 。

隐私权政策

所有应用都必须在 Play 管理中心的指定字段中发布隐私权政策链接，并在应用内发布隐私权政策链接或文本。隐私权政策（以及任何形式的应用内披露声明）必须详尽地说明您的应用如何访问、收集、使用和分享用户数据，不限于“数据安全”部分中披露的数据。隐私权政策必须包含：

- 开发者信息，以及隐私权问题联系人或咨询机制。
- 披露应用将访问、收集、使用和分享哪些类型的个人数据和敏感用户数据以及这些数据的所有分享对象。
- 关于个人数据和敏感用户数据的安全数据处理流程。
- 开发者的数据保留和删除政策。
- 清晰标示隐私权政策（例如，在标题中列示“隐私权政策”字样）。

应用的 Google Play 商品详情中提到的实体（例如开发者、公司）必须出现在隐私权政策中，或应用名必须出现在隐私权政策中。不访问任何个人数据及敏感的用户数据的应用也必须提交隐私权政策。

请确保您的隐私权政策能够通过可公开访问且未设定地理围栏的有效网址（非 PDF）查看，且不可编辑。

帐号删除要求

如果您的应用允许用户在应用内创建帐号，则还必须允许用户请求删除他们的帐号。必须为用户提供易于发现的选项，以便在应用内和应用外（例如，通过访问您的网站）启动应用帐号删除操作。必须在 Play 管理中心的指定网址表单字段中输入指向此网站资源的链接。

当您根据用户的请求删除应用帐号时，还必须删除与该应用帐号相关联的用户数据。暂时禁用、停用或“冻结”应用帐号不等同于删除帐号。如果您因安全、欺诈防范或法规遵从等正当理由而需要保留某些数据，则必须明确告知用户您的数据保留做法（例如，在隐私权政策中明确告知）。

如需详细了解帐号删除政策要求，请参阅这篇帮助中心文章。如需详细了解如何更新您的数据安全表单，请访问这篇文章。

应用组 ID 的使用

Android 将引入一种新的 ID 来为分析和防欺诈等基本用例提供支持。此 ID 的使用条款如下。

- **用途**：应用组 ID 不得用于广告个性化和广告效果衡量。
- **与个人身份信息或其他标识符的关联**：不得出于广告目的将应用组 ID 与任何 Android 标识符（例如 AAID）或任何个人和敏感数据相关联。
- **透明度和用户意见征求**：您必须通过符合法律规范的隐私权声明（包括您的隐私权政策）向用户披露对应用组 ID 的收集和使用行为，以及对于这些条款的遵从义务。在需要时，您必须征得用户具有法律效力的同意。如需详细了解我们的隐私保护标准，请参阅“用户数据”政策 。

欧盟-美国、英国和瑞士数据隐私权框架

如果您访问、使用或处理通过 Google 获取、能用以直接或间接识别个人且来源于欧洲经济区、英国或瑞士的个人信息（以下简称“欧盟个人信息”），则必须做到以下几点：

- 遵守所有有关隐私、数据安全和数据保护的适用法律、法令、法规和规定；
- 按照欧盟个人信息的相关当事人所同意的用途来访问、使用或处理欧盟个人信息；
- 采取适当的管理措施和技术措施保护欧盟个人信息，避免个人信息丢失或遭到滥用、未经授权或非法的访问、披露、篡改和损毁；并且
- 提供数据隐私权框架原则 所要求的同等保护力度，或 Google 控制方-控制方数据保护条款中所述的适用传输机制。

您必须定期监控自己对这些条件的遵从情况。一旦您无法满足（或很可能将无法满足）这些条件，您必须立即发送电子邮件至 data-protection-office@google.com 通知我们，同时立即停止处理欧盟个人信息，或者采取合理、适当的措施来恢复应有的保护级别。

敏感信息访问权限和 API

向用户提出的敏感信息访问权限和 API 请求必须合理。您所提出的敏感信息访问权限和 API 请求必须对于实现您在 Google Play 商品详情中宣传的现有应用功能或服务来说必不可少。您不得将能够获取用户数据或设备数据的敏感信息权限和 API 用于未披露、未实现或未经许可的功能或用途。此外，不得出于推动销售的目的，出售或分享利用敏感信息访问权限或 API 获取的个人数据或敏感数据。

如果您的应用需要获取敏感数据，请在用户执行相关操作时发出敏感信息访问权限和 API 请求（通过渐进式请求方式），让用户了解该应用需要相关权限的原因。仅将数据用于用户同意的用途。如果您日后想将数据用于其他用途，则必须征求用户意见，并确保用户明确同意这些新增用途。

受限权限

除上述内容外，受限权限是被指定为危险 权限、特殊 权限或签名 权限的那些权限或下面记录的权限。这些权限还受以下额外要求和限制的约束：

- 通过受限权限访问的用户或设备数据视为个人数据和敏感用户数据。用户数据政策 的相关要求适用于这些数据。
- 如果用户拒绝授予受限权限，请尊重其决定；不得操纵或强迫用户同意授予非关键权限。您必须采取合理措施，尽量让未授予敏感权限的用户也能正常使用应用（例如，如果用户限制访问其通话记录，则允许其手动输入电话号码）。
- 明确禁止以违反 Google Play 恶意软件政策 的方式使用权限（包括滥用超出规定的权限的行为 ）。

某些受限权限还可能受下方所述其他要求的约束。这些限制旨在保护用户隐私。在极少数情况下，如果应用提供的功能极具吸引力或相当重要，而该功能只有在获得受限权限后才能实现，我们可能会允许极少数特例，允许其不必遵守下述要求。我们会审查特例申请，评估其在隐私权或安全性方面可能会对用户造成的影响。

短信和通话记录权限

短信和通话记录属于用户的个人敏感数据，相关权限使用行为必须遵循个人信息和敏感信息　政策以及下列限制：

受限权限	要求
通话记录权限组（例如 READ_CALL_LOG、WRITE_CALL_LOG、PROCESS_OUTGOING_CALLS）	必须由用户主动将应用注册为设备的默认电话或助理处理程序。
短信权限组（例如 READ_SMS、SEND_SMS、WRITE_SMS、RECEIVE_SMS、RECEIVE_WAP_PUSH、RECEIVE_MMS）	必须由用户主动将应用注册为设备的默认短信或助理处理程序。

如果应用不具备默认短信、电话或助理处理程序功能，就不得在清单（包括清单中的占位文本）中声明需要使用上述权限。此外，只有在用户主动将应用注册为默认短信、电话或助理处理程序的情况下，应用才能向用户提出上述任何权限请求；当应用不再是默认处理程序时，则必须立即停止使用相应权限。如需了解允许的使用情形和例外情况，请访问此帮助中心页面　。

应用只能将权限（及其衍生数据）用于提供已获批准的核心应用功能。核心功能即应用的主要用途，可能包含一组核心性质的功能，这些功能必须均已在应用说明中醒目地载明并宣传。如果失去核心功能，应用就会“损坏”或无法使用。您只能基于提供应用核心功能或服务的目的，转移、分享或许可使用此类数据，不能将此类数据用于任何其他用途（例如改进其他应用或服务、投放广告或营销）。您不得使用其他方法（包括其他权限、API 或第三方来源）衍生属于通话记录或短信相关权限约束范围内的数据。

位置权限

设备位置信息　属于用户的个人敏感数据，与之相关的操作必须遵守个人信息和敏感信息　政策和“后台位置信息”政策以及下列要求：

- 如果应用不再需要利用受位置信息权限（例如 ACCESS_FINE_LOCATION、ACCESS_COARSE_LOCATION、ACCESS_BACKGROUND_LOCATION）保护的数据来提供应用内的现有功能或服务，就不得再使用这些数据。
- 您不得纯粹出于广告投放或数据分析目的而请求用户授予位置信息权限。如果应用在此类数据的许可用途基础上额外将其用于广告投放目的，则必须遵守我们的广告政策　。
- 即使是为了提供现有功能或服务而需要使用位置信息，应用也应请求最小范围的必要权限（即请求获取粗略位置信息而非精确位置信息、前台权限而非后台权限），并且为相应功能或服务所请求的位置权限级别应在用户的合理预期范围内。例如，如果应用请求在后台获取位置信息或有此获取行为，但理由缺乏说服力，我们可能会拒绝该应用。
- 在后台获取的位置信息仅可用于提供对用户有益及与应用核心功能相关的功能。

如果应用仅有前台使用权（例如“在使用时”），则可以使用前台服务权限获取位置信息，前提是：

- 使用此权限是为了完成用户在应用内发起的操作的后续操作；并且
- 此权限使用行为会在应用完成与用户所发起操作相对应的预期使用情形后立即终止。

专门为儿童设计的应用必须遵守亲子同乐计划　政策。

如需详细了解政策要求，请参阅这篇帮助文章　。

所有文件访问权限

用户设备上的文件和目录属性属于用户的个人敏感数据，相关权限使用行为必须遵循个人信息和敏感信息　政策以及下列要求：

- 应用应仅请求访问对其运行至关重要的设备存储空间，而不得出于与面向用户提供的关键应用功能无关的目的，代表任何第三方请求访问设备存储空间。
- 搭载 Android R 或更高版本的 Android 设备要求有 MANAGE_EXTERNAL_STORAGE 权限才能管理对共享存储空间的访问权限。如果应用以 Android R 为目标平台并请求获得对共享存储空间的广泛访问权限（“所有文件访问权限”），则必须在发布前成功通过相应的访问权限审核。若应用获准使用此权限，还必须明确提示用户在“特殊应用权限”设置下为其应用启用“所有文件访问权限”。如需详细了解 Android R 版本的要求，请参阅这篇帮助文章 。

软件包（应用）查看权限

从设备上查询到的已安装应用目录信息属于个人数据和敏感用户数据，与之相关的操作必须遵守个人信息和敏感信息 政策以及下列要求：

如果应用的核心用途是启动、搜索设备上的其他应用或与其他应用进行互操作，则该应用可针对设备上所安装的其他应用获取适当范围的可见性权限，具体如下所述：

- **广泛的应用可见性**：广泛的可见性是指应用对设备上所安装的应用（“软件包”）具有大范围的（“广泛的”）发现权限。
  - 如果应用以 API 级别 30 或更高级别 为目标环境，则该应用通过 QUERY_ALL_PACKAGES 权限所获得的针对已安装应用的广泛可见性仅可用于如下特定使用情形：应用需要知晓设备上安装的任何应用或所有应用，并且/或者要与之进行互操作，才能正常发挥作用。
    - 如果应用使用范围更具体的软件包可见性权限声明 （例如，查询特定软件包并与之互动，而不是请求广泛的可见性权限）即可正常运作，那么该应用不得使用 QUERY_ALL_PACKAGES 权限。
  - 如果应用通过其他方法获取的权限近似于与 QUERY_ALL_PACKAGES 权限关联的广泛可见性级别权限，那么这种权限也仅限用于面向用户的核心应用功能以及与通过该方法发现的应用进行的互操作。
  - 如需了解 QUERY_ALL_PACKAGES 权限的允许使用情形，请参阅这篇帮助中心文章 。
- **有限的应用可见性**：有限的可见性是指应用利用更具针对性的（而不是“广泛的”）方法查询特定应用（例如，查询与您的应用清单声明相符的特定应用），从而最大限度地减少数据访问。如果应用能够以符合政策的方式与其他应用进行互操作或管理这些应用，则该应用可以利用此方法来查询这些应用。
- 您的应用对设备上所安装应用的目录信息的可见性权限必须与用户在您的应用中要实现的核心目的或使用的核心功能直接相关。

通过 Play 分发的应用所查询的应用目录数据不得出售，也不得分享给其他方用于分析或广告变现目的。

无障碍功能 API

无障碍功能 API 不能用于：

- 在未经用户许可的情况下更改用户设置或是不让用户停用或卸载任何应用或服务，除非家长或监护人通过家长控制应用授权，或者已获授权的管理员通过企业管理软件授权；
- 规避 Android 内置的隐私控制机制和通知；
- 以具有欺骗性或违反 Google Play 开发者政策的方式更改或利用界面。

Accessibility API 不应用于远程通话录音，应用也不得向该 API 发出此类请求。

必须在 Google Play 商品详情中注明无障碍功能 API 的使用情形。

关于 IsAccessibilityTool 的指南

如果应用的核心功能旨在直接为残障人士提供支持，这些应用可以使用 **IsAccessibilityTool**，从而以适当方式公开宣称自身为无障碍应用。

如果应用不符合 **IsAccessibilityTool** 的使用条件，则不得使用该标记，且必须满足“用户数据”政策 中所述的“关于提供醒目披露声明与征求用户同意的要求”，因为应用中的无障碍相关功能往往不是显而易见的。如需了解详情，请参阅 AccessibilityService API 帮助中心文章。

应用必须尽可能使用范围更小的 API 和权限 来替代无障碍功能 API，以实现所需功能。

请求安装包权限

若应用取得 REQUEST_INSTALL_PACKAGES 权限，则可以请求安装应用软件包。若要使用该权限，应用的核心功能必须包括以下操作：

- 发送或接收应用软件包；
- 启动由用户发起的应用软件包安装流程。

许可的功能包括：

- 浏览或搜索网页
- 支持附件的通信服务
- 文件共享、传输或管理
- 企业设备管理
- 备份和恢复
- 设备间迁移/手机间传输
- 用于将手机同步到穿戴式设备或 IoT 设备（例如智能手表或智能电视）的配套应用

核心功能是指应用的主要用途。您必须在应用说明中醒目地载明并强调核心功能以及构成核心功能的所有核心特性。

REQUEST_INSTALL_PACKAGES 权限不得用于执行自我更新、修改或在资源文件中捆绑其他 APK，除非是出于设备管理目的。所有更新或软件包安装操作都必须遵守 Google Play 的“设备和网络滥用”政策，并且必须由用户发起和推进。

“身体传感器”权限

用于衡量身体生理参数的传感器数据（例如心率、血氧饱和度和体表温度）会被视为用户个人数据和敏感用户数据。请求访问此类数据的应用都必须遵守“用户数据”政策和“健康类应用”政策中所述的要求。这适用于所有类型的设备（包括手机、平板电脑和 Wear OS 设备）中对 `android.permission.BODY_SENSORS` 和 `android.permission.BODY_SENSORS _BACKGROUND` 权限的请求。

自 Android 16 起，宽泛的 `BODY_SENSORS` 权限让位于针对具体数据类型且更可保护隐私的精细 `android.permissions.health.*` 权限（例如 `android.permission.health.READ_HEART_RATE`、`android.permission.health.READ_OXYGEN_SATURATION`、`android.permission.health.READ_SKIN_TEMPERATURE`）。

凡是以 Android 16 或更高版本为目标平台的应用，都必须使用这些具体的权限才能访问之前要求应用具有 `BODY_SENSORS` 权限的 API。如需了解完整详情，请参阅行为变更：以 Android 16 或更高版本为目标平台的应用页面。

所有对“身体传感器”权限（无论是旧版权限还是新版精细权限）的请求都会被审核，以确保此类个人数据和敏感数据的预期用途与会让用户直接受益的获批使用情形一致。获批使用情形主要涉及健身与健康监测功能（例如实时锻炼监控）、医疗或病症监控、健康调研（需获得相应批准）或穿戴式设备配套应用增强功能。

如需获取综合指南，包括禁止的用途、可接受的使用情形和详细的要求，请参阅 Android 健康权限：指南和常见问题解答。

Health Connect by Android 权限

健康数据共享 是一个 Android 平台，可以让健康与健身应用在统一的生态系统内存储和共享相同的设备端数据。此外，用户只需通过这一个平台，即可控制哪些应用能够读取和写入自己的健康与健身数据，包括健康记录。健康记录可能涵盖病史、诊断信息、治疗方案、用药记录、检验结果以及其他临床数据，这些数据通常由医疗服务提供方或机构提供，或者通过受支持的第三方健康平台获取。

“健康数据共享”支持读取和写入各种类型的数据 ，从步数到体温，再到健康记录数据，均在此列。

通过“健康数据共享”权限访问的数据属于用户个人数据及敏感用户数据，使用这些数据时必须遵循“用户数据”政策。如果您的应用属于健康类应用，或提供健康相关功能并会访问健康数据（包括“健康数据共享”数据），则该应用必须遵守“健康类应用”政策。

请参阅这份 Android 开发者指南 ，了解如何开始使用“健康数据共享”。如需获取访问“健康数据共享”相关类型数据的权限或查看其他常见问题解答，请参阅 Android 健康权限：指南和常见问题解答。

通过 Google Play 分发的应用必须符合以下政策要求，才能在“健康数据共享”中读取和/或写入数据。

以适当的方式访问和使用 Health Connect

使用“健康数据共享”时必须遵守适用的政策、条款及条件，并且符合本政策中规定的获批使用情形。也就是说，只有当应用或服务符合其中一种获批使用情形时，您才能请求使用相应权限。

获批使用情形包括：健身和健康、奖励、健身指导、公司健康计划、医疗护理、健康研究，以及游戏。获准用于这些使用情形的应用不得将其使用情形扩展至未披露或未经允许的用途。

仅当应用或服务的一项或多项功能的设计目的是帮助用户开展有益的健康与健身活动时，应用或服务才能请求使用“健康数据共享”权限。具体包括：

- 应用或服务允许用户**直接记录、报告、监控和/或分析**自己的身体活动、睡眠状况、心理健康状况、营养状况、健康测量结果、身体特征说明、健康记录和/或其他与健康或健身相关的说明和测量结果。
- 应用或服务允许用户在设备上**存储自己的身体活动记录、睡眠状况、心理健康状况、营养状况、健康测量结果、身体特征说明、健康记录**和/或其他与健康或健身相关的说明和测量结果，并将数据共享给设备上符合这些使用情形的其他应用。
- 应用或服务允许用户管理慢性疾病、医疗或护理支持。

使用“健康数据共享”权限时不得违反本政策，也不得违反其他适用的“健康数据共享”条款及条件或政策，包括不得将该权限用于实现以下目的：

- 如果可以合理预见到，在应用、环境或活动中使用“健康数据共享”或相关故障可能会导致人员伤亡、个体损害、环境破坏或财产损失，则不得将“健康数据共享”用于开发此类应用、环境或活动，也不得将其纳入此类应用、环境或活动中（例如建设或操作核设施、空中交通管制系统、生命支持系统或武器）。
- 不得使用无头应用访问通过“健康数据共享”获取的数据。应用必须在应用托盘、设备配套应用的设置界面、通知图标等位置显示清晰可辨的图标。
- 如果应用在不兼容的设备和平台之间同步数据，则不得与“健康数据共享”一起使用。
- 不得将“健康数据共享”用于连接仅面向儿童的应用、服务或功能。
- 采取合理且适当的措施来保护使用“健康数据共享”的所有应用或系统，以免遭到未经授权或非法的访问、使用、损坏、损失、篡改或披露。

此外，在将“健康数据共享”及“健康数据共享”中的任何数据用于预期用途时，您还有责任确保遵守可能适用的任何法规或法律要求。例如，如果您是受《健康保险流通与责任法案》(HIPAA) 约束的实体或业务伙伴，就必须恪守与访问和使用“健康数据共享”信息相关的适用要求。同样，如果您是受面向欧盟用户的《一般数据保护条例》(GDPR) 约束的开发者，则必须履行 GDPR 规定的义务。这些法律法规可能会要求您，在将数据共享给参与您的处理活动的相关实体之前签署额外协议，比如《业务伙伴协议》或《数据处理协议》。此外，应用开发者还应负责确定，是否需要签署这类协议才能开展其活动。收到要求后，开发者必须向 Google 提供已签署此类协议或活动合规的证明。

除非 Google 在针对特定 Google 产品或服务提供的标签或信息中明确指明，否则 Google 不为将“健康数据共享”中包含的任何数据用于任何用途或目的（尤其是研究、健康或医疗用途）的行为背书，也不保证这些数据的准确性。对于使用通过“健康数据共享”获取的数据的行为，Google 概不承担任何相关法律责任。

有限使用

访问和使用“健康数据共享”数据时，须遵守特定限制条件：

- 数据只能用于提供或改进适当的使用情形或应用界面中显示的功能。
- 只有在用户明确同意且满足以下条件的情况下，才能将用户数据传输给第三方：出于安全目的（例如，调查滥用行为）、符合适用的法律或法规，或者因组织合并/收购而需要传输这类数据。
- 除非满足以下条件，否则限制人为访问用户数据的行为：已获得用户的明确同意、出于安全目的、符合适用的法律规定，或者按照法律要求汇总数据以供内部运营之用。
- **禁止任何其他传输、使用或出售“健康数据共享”数据的行为，包括：**
  - 向第三方（如广告平台、数据代理商或任何信息转销商）传输或出售用户数据。

- 以投放广告（包括投放个性化广告或针对用户兴趣投放广告）为目的传输、出售或使用用户数据。
- 以确定用户的信誉度或进行贷款为目的传输、出售或使用用户数据。
- 通过可能被认定为医疗设备的任何产品或服务传输、出售或使用用户数据，除非相应医疗设备应用遵守所有适用的法规，包括已事先获得相关监管机构（如美国食品药品监督管理局）的必要官方许可或批准，表明可以将“健康数据共享”数据用于预期用途，并已就此征得用户的明确同意。
- 出于任何目的或通过任何方式传输、出售或使用涉及受保护健康信息（如《健康保险流通与责任法案》[HIPAA] 中所定义）的用户数据，除非相应行为是由用户发起的且符合 HIPAA 规定。

请求最小范围的权限

您只能请求获取实现产品功能或服务所必需的权限。此类权限请求应仅针对且仅限于必要的数据。

透明且准确的通知和控制措施

“健康数据共享”会处理健康与健身数据，包括个人信息和敏感信息。开发者必须制定详尽全面的隐私权政策，将其在数据方面的做法以清晰且易于获取的方式披露给用户。这类披露必须包括：

- 如实表明请求访问用户数据的应用或服务的身份。
- 清晰、准确地阐述正在访问、请求和/或收集的数据类型。这些数据必须与应用内面向用户提供的功能或建议紧密相关。
- 说明数据的使用和/或共享方式：如果您出于某种原因请求数据，但也会将数据用于另一目的，则必须向用户全面披露所有使用情形。
- 提供用户帮助文档，指导用户如何在应用内管理和删除其数据，并说明在停用和/或删除账号时数据的处理情况。
- 阐明如何以安全的方式处理所有用户个人数据和敏感用户数据，包括使用新型加密技术（例如通过 HTTPS）传输数据。

如需详细了解与关联“健康数据共享”的应用相关的要求，请参阅这篇帮助中心文章。

VPN 服务

VpnService 是供应用扩展和构建自己的 VPN 解决方案的基类。只有使用 VpnService 并将 VPN 作为其核心功能的应用才能创建指向远程服务器的安全设备级隧道。例外情况包括需要远程服务器来实现核心功能的应用，例如：

- 家长控制和企业管理应用。
- 应用使用情况跟踪。
- 设备安全性应用（例如防病毒、移动设备管理、防火墙）。
- 与网络相关的工具（例如远程访问）。
- 网络浏览应用。
- 需要利用 VPN 功能来提供电话或连接服务的运营商应用。

VpnService 不能用于：

- 在未提供醒目披露声明和未征得用户同意的情况下收集个人数据和敏感用户数据。
- 出于变现目的重定向或操控来自某个设备上其他应用的用户流量（例如，重定向广告流量，使之流经与用户所在国家/地区不同的国家/地区）。

使用 VpnService 的应用必须：

- 在 Google Play 商品详情中注明 VpnService 的使用情形；
- 必须加密从设备到 VPN 隧道端点的数据；
- 遵守所有开发者计划政策 ，包括广告欺诈 、权限 和恶意软件 政策。

精确闹钟权限

系统将引入一个新的权限 USE_EXACT_ALARM，用于向以 Android 13（目标 API 级别 33）或更高版本为目标平台的应用授予对精确闹钟功能 的访问权限。

USE_EXACT_ALARM 是一项受限权限，应用只有在其核心功能支持精确闹钟需求的情况下才能声明此权限。请求此受限权限的应用需要接受审核；如果应用不符合可接受的用例标准，则不允许在 Google Play 上发布。

使用精确闹钟权限的可接受用例

仅当应用面向用户的核心功能需要精确计时的操作时，应用才必须使用 USE_EXACT_ALARM 功能，例如：

- 应用是闹钟或计时器应用。
- 应用是显示事件通知的日历应用。

如果您有上文未涵盖的精确闹钟功能用例，则应评估能否选择使用 SCHEDULE_EXACT_ALARM 作为替代方案。

如需详细了解精确闹钟功能，请参阅此开发者指南 。

全屏 intent 权限

对于以 Android 14（API 目标级别 34）及更高版本为目标平台的应用，USE_FULL_SCREEN_INTENT 是一项特殊应用访问权限 。只有当应用的核心功能属于以下需要高优先级通知的类别之一时，系统才会自动授权应用使用 USE_FULL_SCREEN_INTENT 权限：

- 设置闹钟
- 接听来电或视频通话

请求此权限的应用需要接受审核；如果应用不符合上述条件，系统将不会自动向其授予此权限。在这种情况下，应用必须向用户请求权限，才能使用 USE_FULL_SCREEN_INTENT。

特此提醒，任何使用 USE_FULL_SCREEN_INTENT 权限的行为均必须遵循所有 Google Play 开发者政策，其中包括我们的移动垃圾软件政策、设备和网络滥用政策以及广告政策。全屏 intent 通知不得干扰、中断、损害或以未经授权的方式访问用户的设备。此外，应用不得妨碍其他应用或设备的易用性。

如需详细了解 USE_FULL_SCREEN_INTENT 权限，请访问我们的帮助中心。

设备和网络滥用

我们不允许应用干扰、中断、损害或以未经授权的方式访问用户的设备、其他设备/计算机、服务器、网络、应用编程接口 (API) 或服务，包括但不限于相应设备上的其他应用、任何 Google 服务或授权运营商的网络。

Google Play 上的应用必须符合 Google Play 核心应用质量指南 中列出的默认 Android 系统优化要求。

对于通过 Google Play 分发的应用，不得采用 Google Play 更新机制以外的其他任何方式修改、替换或更新应用本身。同样地，应用不得从 Google Play 以外的来源下载可执行代码（例如 dex、JAR 和 .so 文件）。这项限制不适用于在虚拟机或解释器中运行且通过这种方式间接访问 Android API 的代码（例如 WebView 或浏览器中的 JavaScript）。

如果应用或第三方代码（例如 SDK）会在运行时加载 JavaScript、Python 或 Lua 等解释型语言（例如，未打包到应用软件包中的此类代码），不得允许发生可能违反 Google Play 政策的行为。

我们不允许任何代码引入或利用安全漏洞。查看应用安全性改进计划 ，了解应用开发者需注意的最新安全问题。

下面是常见违规行为的一些示例：

“设备和网络滥用”常见违规行为示例：

- 应用阻止或干扰其他应用展示广告。
- 应用用于游戏作弊，影响到其他应用的游戏内容。

- 应用为入侵服务、软件或硬件或者规避安全保护措施提供便利或相关操作说明。
- 应用以违反服务条款的方式访问或使用特定服务或 API。
- 应用不符合加入许可名单的条件 ，却试图绕过系统电源管理机制 。
- 应用帮助向第三方提供代理服务；但如果该服务是应用面向用户提供的主要核心功能，则不构成违规。
- 应用或第三方代码（例如 SDK）从 Google Play 以外的来源下载可执行代码（例如 dex 文件或原生代码）。
- 应用事先未经用户同意便在设备上安装其他应用。
- 应用为分发或安装恶意软件提供链接或便利。
- 应用或第三方代码（例如 SDK）包含具有额外 JavaScript 接口的 WebView，并且该接口会加载不受信任的网络内容（例如 http:// 网址）或从不受信任的来源获取的未经验证的网址（例如，通过不受信任的 intent 获取的网址）。
- 应用利用全屏 intent 权限 强制用户与干扰性广告或通知进行互动。
- 应用通过规避 Android 沙盒保护 ，从其他应用中获取用户活动信息或用户身份信息。

前台服务使用

前台服务权限可确保正确使用面向用户的前台服务。对于以 Android 14 及更高版本为目标平台的应用，您必须为应用中使用的每项前台服务指定有效的前台服务类型，并为该类型声明适当的前台服务权限。例如，如果应用所使用的前台服务需要使用地图地理定位功能，您必须在应用的清单中声明 FOREGROUND_SERVICE_LOCATION 权限。

只有在前台服务的使用满足以下条件时，应用才可以声明前台服务权限：

- 提供对用户有益且与应用核心功能相关的功能
- 由用户发起或用户可感知（例如，播放歌曲的音频、将媒体投放到其他设备、准确清晰的用户通知、用户请求将照片上传到云端）
- 可以由用户终止或停止
- 不可被系统中断或延迟，否则会导致负面用户体验，或导致用户预期的功能无法正常运行（例如，通话必须立即开始，且不可被系统延迟）。
- 只在完成任务所需的时间内运行

以下前台服务的使用情形不受上述条件约束：

- 前台服务类型 systemExempted 或 shortService ；
- 前台服务类型 dataSync（仅限使用 Play Asset Delivery 功能时）

有关如何使用前台服务的详细说明，请访问此处。

用户发起的数据传输作业

只有在使用情形满足以下条件时，应用才能使用 User-Initiated Data Transfer Jobs API：

- 由用户发起
- 用于网络数据传输任务
- 只在完成数据传输所需的时间内运行

有关如何使用 User-Initiated Data Transfer API 的详细说明，请访问此处。

与 FLAG_SECURE 相关的要求

FLAG_SECURE 是一个在应用代码中声明的屏幕标记，用于表明应用界面 (UI) 包含敏感数据，且这些数据仅限于在使用应用时通过安全的途径使用。此标记旨在防止此类数据显示在屏幕截图中或通过不安全的屏幕查看。如果应用内容不应在应用或用户设备以外进行广播、查看或以其他方式传输，开发者会声明此标记。

出于安全和隐私保护的目的，所有在 Google Play 上分发的应用都必须遵守其他应用的 FLAG_SECURE 声明。也就是说，应用不得帮助或创建权变措施来绕过其他应用中的 FLAG_SECURE 设置。

符合无障碍工具 条件的应用不受此要求的约束，前提是此类应用不会传播、保存或缓存受 FLAG_SECURE 保护的内容，以用于在用户设备之外进行访问。

运行设备端 Android 容器的应用

设备端 Android 容器应用会提供模拟全部或部分底层 Android 操作系统的环境。这些环境中的体验可能不会反映全套 Android 安全功能 ，因此开发者可以选择添加安全环境清单标志，以便向设备端 Android 容器表明，这些容器不得在其模拟的 Android 环境中运作。

安全环境清单标志

REQUIRE_SECURE_ENV 是一个可以在应用的清单中声明的标志，用于指明相应应用不得在设备端 Android 容器应用中运行。出于安全和隐私保护的目的，提供设备端 Android 容器的应用必须尊重声明了此标志的所有应用，并且：

- 查看应用清单，确认要在设备端 Android 容器中加载的应用是否声明了此标志。
- 切勿将声明了此标志的应用加载到其设备端 Android 容器中。
- 不得充当代理，即不得通过在设备上拦截或调用 API，使它们看起来像是安装在容器中。
- 不得为绕过此标志提供便利或创建解决方法（例如，通过加载版本较低的应用，来绕过当前应用的 REQUIRE_SECURE_ENV 标志）。

您可以访问我们的帮助中心，详细了解此政策。

欺骗性行为

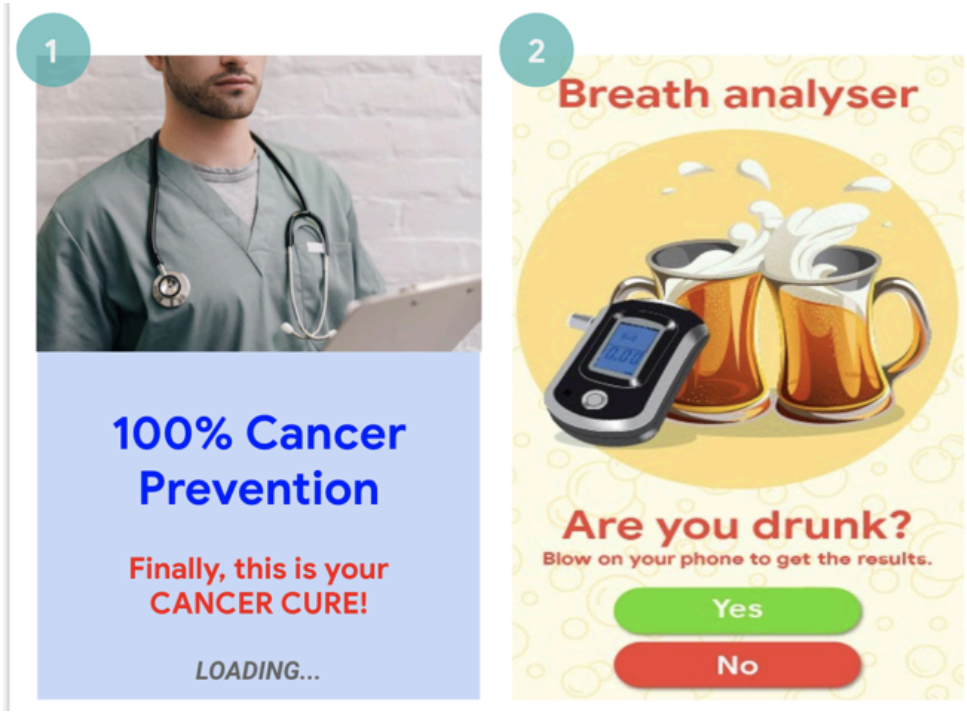
我们不允许任何应用试图欺骗用户或协助促成不诚实行为，包括但不限于被判定为功能上无法兑现其承诺的应用。应用必须在其元数据的所有部分中针对自身功能提供准确的声明、说明和相关图片/视频。应用不得试图模仿操作系统或其他应用的功能或警告。对设备设置的任何更改都必须在用户知情并同意的情况下进行，而且必须让用户可以撤消更改。

误导性声明

我们不允许任何应用（包括应用的说明、名称、图标和屏幕截图）中包含虚假或误导性的信息或声明。

下面是常见违规行为的一些示例：

- 应用功能描述不实或未提供准确清晰的功能说明：
  - 应用的说明和屏幕截图表明该应用是竞速游戏，但实际上它却是使用汽车图片的益智拼图游戏。
  - 应用声称是防病毒应用，但却只用一个文本指南来说明如何清理病毒。
- 应用声称提供某些功能（例如，防虫应用），但实际上不可能实现这些功能。即使是以恶作剧、假装、笑话等形式做出这类声明，也属于违规行为。
- 应用分类不当，包括但不限于应用分级或应用类别。
- 应用包含明显具有欺骗性或虚假的内容，相应内容可能会干扰投票过程或歪曲选举结果。
- 应用谎称与政府实体之间存在关联，或者在未经正当授权的情况下谎称提供或协助提供政府服务。
- 应用谎称是某知名实体的官方应用。举例来说，在未获得必要许可或权利的情况下，应用不得使用诸如“贾斯汀·比伯官方应用”之类的标题。



(1) 此应用包含具有误导性的医疗或健康相关声明（如治愈癌症）。
(2) 此应用声称可提供某些不可能实现的功能（如将手机用作呼气酒精测量仪）。

以欺骗性手段更改设备设置

我们不允许任何应用在用户不知情或未许可的情况下，更改用户设备上超出该应用范围的设置或功能。设备设置和功能包括系统和浏览器设置、书签、快捷方式、图标、微件以及主屏幕上应用的呈现方式。

此外，我们也不允许以下行为：

- 应用在征得用户同意后修改设备设置或功能，但未向用户提供简单的方式来撤消所做更改。
- 应用或广告修改设备设置或功能，以此作为向第三方提供的服务或借此达成广告宣传目的。
- 应用误导用户移除或停用第三方应用或者修改设备设置或功能。
- 应用鼓动或诱导用户移除或停用第三方应用或者修改设备设置或功能，除非该应用属于具有公信力的安全服务。

促成不诚实行为

我们不允许任何应用以任何方式协助用户误导他人或提供用于实现欺骗性行为的功能，包括但不限于生成或协助生成身份证、社会保障号、护照、文凭、信用卡、银行账户和驾照。应用必须针对自身的功能和/或内容提供准确的声明、名称、说明和相关图片/视频，并按用户合理预期的方式运行。

附加应用资源（例如游戏资产）只有作为用户使用应用的必需资源时才可供下载。下载的资源必须符合所有 Google Play 政策，并且在下载开始之前，应用应提示用户并明确声明所下载资源的大小。

即使应用声称是“恶作剧”或“纯属娱乐”（或其他类似描述），也仍须遵守我们的政策要求。

下面是常见违规行为的一些示例：

- 应用冒充其他应用或网站来骗取用户的个人信息或身份验证信息。
- 应用未经相关个人或实体同意即描述或显示未经验证或真实的电话号码、联系信息、地址或个人身份信息。
- 应用根据用户的地理位置、设备参数或其他与用户相关的数据而提供不同核心功能，但未在商品详情中向用户突出说明这些不同差异。
- 在未提醒用户（例如在“新功能”部分　中加以说明）并更新商品详情的情况下，应用版本之间发生重大变更。
- 应用尝试在审核期间修改或混淆某些行为。

- 采用内容分发网络 (CDN) 的应用会下载相关内容，但在下载之前不会提示用户并声明所下载资源的大小。

操纵媒体内容

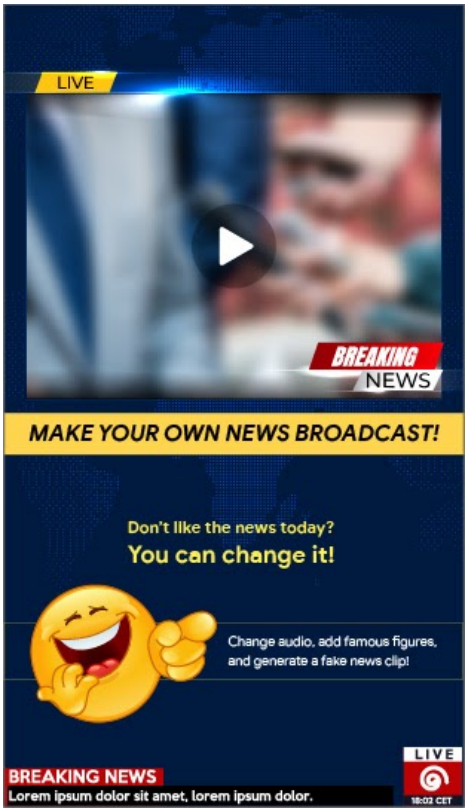
我们不允许任何应用宣传或协助创建通过图像、音频、视频和/或文字传达的虚假或误导性信息或声明。我们禁止发布被判定为宣传以下媒体内容或使其长久存续的应用：明显具有误导性或欺骗性且可能会造成严重危害（牵涉敏感事件、政治、社会问题或其他引起公众关注的问题）的图像、视频和/或文字。

如果内容符合公共利益、图像明显是人造的、被操纵的媒体内容带有面向用户的免责声明或水印，或者内容具有明显的讽刺或滑稽模仿意味，我们可能会给予例外处理。

被操纵的媒体内容必须遵守现有的 Google Play 开发者政策，包括不得发布被受限内容政策禁止的内容。

下面是常见违规行为的一些示例：

- 应用使用公众人物或与敏感事件相关的媒体内容在应用的商品详情中宣传媒体修改功能。
- 应用能够修改媒体剪辑，通过在其中添加真实新闻媒体的名称或徽标（但没有明晰的免责声明或水印），来模仿新闻广播。
- 应用的唯一目的是创建误导性媒体内容。



(1) 通过此应用提供的功能，用户可以修改媒体剪辑来模仿新闻广播，并可在不加水印的情况下将名人或公众人物添加到剪辑中。

行为透明度

对普通用户而言，应用功能应清楚明了；应用中应不包括任何隐藏的、休眠的或未载明的功能。我们禁止使用可用于规避应用审查的技术。应用可能需要提供额外的详细信息，以确保用户安全、系统完整性和政策遵从性。

不实陈述

我们不允许应用或开发者帐号有以下行为：

- 冒充任何个人或组织，或者虚报或隐瞒其所有权或主要目的。

- 从事刻意误导用户的活动。这包括但不限于有以下行为的应用或开发者帐号：谎报或隐瞒其源自哪个国家/地区，以及将内容定向到另一国家/地区的用户。
- 在应用的内容与政治、社会问题或公众关注话题相关的情况下，与其他应用、网站、开发者或帐号合作，以隐瞒或谎报开发者身份、应用身份或其他重大详细信息。

Google Play 的目标 API 级别政策

为了向用户提供安全可靠的使用体验，Google Play 要求**所有应用**遵守以下目标 API 级别要求：

新应用和应用更新的目标 API 级别必须为最新的主要 Android 版本发布日期前一年内推出的 Android API 级别。不符合此要求的新应用和应用更新将无法在 Play 管理中心提交。

对于**未更新的现有 Google Play 应用**，如果其目标 API 级别不是最新的主要 Android 版本发布日期前两年内推出的 API 级别，则无法提供给设备运行较新版 Android 操作系统的新用户。之前从 Google Play 安装过相应应用的用户仍可以在应用支持的任何 Android 操作系统版本中发现、重新安装和使用该应用。

如需获取有关如何满足目标 API 级别要求的技术建议，请参阅迁移指南 。

如需了解确切的时间表和例外情况，请参阅这篇帮助中心文章 。

用户数据政策

您必须清楚说明您的应用会如何处理用户数据（例如从用户那里收集到的信息或与用户相关的信息，包括设备信息）。也就是说，您必须披露应用访问、收集、使用、处理以及分享用户数据的方式，并且仅将这些数据用于已披露的合规用途。

如果您的应用中包含第三方代码（例如 SDK），那么您必须确保应用中使用的第三方代码，以及相应第三方对应用中用户数据的处理做法，均符合 Google Play 开发者计划政策，包括使用要求和信息披露要求。例如，您必须确保 SDK 提供方不会出售应用中的用户个人数据和敏感用户数据。无论用户数据是在发送到服务器后进行传输，还是通过在应用中嵌入第三方代码进行传输，此要求都适用。

用户个人数据和敏感用户数据

- 仅当应用和服务功能以及合规用途在用户的合理预期范围内，才可以访问、收集、使用和分享通过应用获取的用户个人数据和敏感用户数据：
  - 如果应用还将用户个人数据和敏感用户数据用于广告投放，则必须遵守 Google Play 的“广告”政策。
- 以安全的方式处理所有用户个人数据和敏感用户数据，包括使用新型加密技术（例如通过 HTTPS）来传输数据。
- 在访问受 Android 权限控制的数据之前，应尽可能使用运行时权限请求。

用户个人数据和敏感用户数据的出售

不得出售用户个人数据和敏感用户数据。

- “出售”是指以获得金钱为目的，将用户个人数据和敏感用户数据交换或传输给第三方。
  - 用户发起的用户个人数据和敏感用户数据传输行为不视为出售（例如，用户使用应用的某项功能将文件传输给第三方，或用户选择使用专用的调研应用）。

关于提供醒目披露声明和征求用户同意的要求

如果您的应用对用户个人数据和敏感用户数据的访问、收集、使用或分享方式不在用户对相应产品或功能的合理预期范围内，您必须满足用户数据政策中关于提供醒目披露声明和征求用户同意的要求。

如果您的应用集成了旨在默认收集用户个人数据和敏感用户数据的第三方代码（例如 SDK），那么您必须在收到 Google Play 要求后的 2 周内（或者，如果 Google Play 的要求提供了更长的期限，则以相应期限为准）提供足够的证据，证明您的应用符合本政策中关于提供醒目披露声明和征求用户同意的要求，包括关于通过第三方代码访问、收集、使用或分享数据的要求。

请务必确保您对第三方代码（例如 SDK）的使用不会导致您的应用违反用户数据政策。

如需详细了解关于提供醒目披露声明和征求用户同意的要求，请参阅这篇帮助中心文章。

SDK 导致的违规行为示例

- 应用使用 SDK 收集用户个人数据和敏感用户数据，但未按照本用户数据政策的要求、数据访问/处理（包括禁止的出售行为）方面的要求，以及关于提供醒目披露声明和征求用户同意的要求来处理这些数据。
- 应用集成的 SDK 默认收集用户个人数据和敏感用户数据，并且收集行为违反此政策中关于提供醒目披露声明和征求用户同意的要求。
- 应用使用的 SDK 声称仅出于为应用提供反欺诈和反滥用功能的目的而收集用户个人数据和敏感用户数据，但实际上还会出于广告投放和分析目的而将收集的数据分享给第三方。
- 应用中的 SDK 会在未遵循醒目披露声明准则和/或隐私权政策指南的情况下，擅自传输有关用户已安装的软件包的信息。
  - 另请参阅“移动垃圾软件”政策。

针对访问个人数据和敏感数据的其他要求

下表介绍了针对特定活动的要求。

活动	要求
您的应用会收集或关联永久性设备标识符，例如 IMEI、IMSI、SIM 卡序列号等	永久性设备标识符不得与其他的用户个人数据和敏感用户数据或可重置的设备标识符关联，以下用途除外： • 用于与 SIM 卡身份信息关联的电话服务（例如与某个运营商账号关联的 Wi-Fi 通话服务）； • 用于以设备所有者模式运行的企业设备管理应用。 您必须按照用户数据政策中的规定以醒目的方式向用户披露以上用途。 如需了解其他唯一标识符，请参阅此资源 。 如需了解 Android 广告 ID 方面的更多指南，请参阅“广告”政策。
您的应用以儿童为目标用户	您的应用只能包含已完成自行认证、可用于儿童服务的 SDK。如需了解所有政策内容及要求，请参阅家庭内容自行认证广告 SDK 计划。

SDK 导致的违规行为示例

- 应用使用的 SDK 关联到 IMEI 和位置信息权限。
- 应用使用的 SDK 会出于任何广告投放或数据分析目的而将 Android 广告 ID (AAID) 关联到永久性设备标识符。
  应用使用的 SDK 会出于数据分析目的而关联 AAID 和电子邮件地址。

“数据安全”部分

所有开发者都必须在每个应用中提供清晰准确的“数据安全”部分，详细说明用户数据的收集、使用和分享方式，其中包括通过应用所用的任何第三方库或 SDK 收集和处理的数据。开发者应负责确保标签的准确性并及时更新相关信息。如适用，“数据安全”部分应与应用的隐私权政策中披露的信息一致。

如需详细了解如何填写“数据安全”部分，请参阅这篇帮助中心文章。

查看完整的用户数据政策。

“敏感信息访问权限和 API”政策

向用户提出的敏感信息访问权限和 API 请求必须合理。您所提出的敏感信息访问权限和 API 请求必须对于实现您在 Google Play 商品详情中宣传的现有应用功能或服务来说必不可少。您不得将能够获取用户数据或设备数据的敏感信息权限和 API 用于未披露、未实现或未经许可的功能或用途。此外，不得出于促销目的，出售或分享利用敏感信息访问权限或 API 获取的个人数据或敏感数据。

查看完整的“敏感信息访问权限和 API”政策。

SDK 导致的违规行为示例

- 应用中的 SDK 会请求在后台获取位置信息，并将其用于不允许或未披露的用途。
- 应用中的 SDK 会在未经用户同意的情况下传输 read_phone_state Android 权限所衍生的 IMEI。

“设备和网络滥用”政策

我们的恶意软件政策很简单：保护 Android 生态系统（包括 Google Play 商店）和用户设备免遭恶意行为（例如恶意软件攻击）侵扰。秉持这一基本原则，我们积极致力于向用户及其 Android 设备提供安全的 Android 生态系统。

恶意软件是指任何可能给用户、用户数据或设备带来风险的代码。恶意软件包括但不限于潜在有害应用 (PHA)、二进制文件或框架修改，所涵盖的类别包括特洛伊木马、钓鱼式攻击和间谍软件应用等。我们会不断更新并添加新类别。

此政策的要求也适用于您在应用中纳入的任何第三方代码（例如 SDK）。

查看完整的“恶意软件”政策。

SDK 造成的違規例子

- 应用包含的 SDK 库来自分发恶意软件的提供方。
- 应用违反 Android 权限模型，或从其他应用窃取凭据（例如 OAuth 令牌）。
- 应用滥用防卸载或防关停功能。
- 应用停用 SELinux。
- 应用中的 SDK 会为了未披露的用途而访问设备数据，获得提升的权限，因而违反了 Android 权限模型。
- 应用中的 SDK 所使用的代码会诱骗用户通过话费代扣方式订阅或购买内容。

在应用内使用 SDK

如果您在应用内添加 SDK，就要负责确保其第三方代码和做法不会导致您的应用违反 Google Play 开发者计划政策。您务必了解应用内的 SDK 如何处理用户数据，并确保了解它们使用哪些权限、收集哪些数据以及这样做的原因。

SDK 要求

应用开发者常常会依赖第三方代码（例如 SDK）为其应用集成关键功能和服务。在应用中添加 SDK 时，您要确保可以保障用户安全并保障您的应用免受任何漏洞的侵害。在本部分中，我们将介绍我们在隐私和安全方面的一些现有要求对 SDK 的约束，以及它们如何有助于开发者安全可靠地将 SDK 集成到应用中。

如果您在应用中添加 SDK，您就要负责确保其第三方代码和做法不会导致您的应用违反 Google Play 开发者计划政策。您务必要了解应用中的 SDK 将如何处理用户数据，并确保您了解它们将使用哪些权限、收集哪些数据，以及这样做的原因。请注意，SDK 对用户数据的收集和处理必须与您的应用对相应数据的合规使用情形一致。

为确保您对 SDK 的使用不违反任何政策要求，请完整阅读和理解下文所述的政策，并注意以下与 SDK 相关的一些现有要求：

未经用户同意取得设备 root 权限的提权应用会被划分为获取 root 权限的应用。

间谍软件

间谍软件是指会收集、泄露或分享与符合政策的功能无关的用户数据或设备数据的恶意应用、代码或行为。

如果恶意代码或行为疑似暗中监视用户，或是未适当通知用户或征得用户同意即泄露数据，亦可视为间谍软件。

查看完整的“间谍软件”政策。

例如，SDK 导致的间谍软件违规行为包括但不限于：

- 应用使用的 SDK 会传输音频或通话录音中的数据，但这与符合政策的应用功能无关。
- 具有恶意第三方代码（例如 SDK）的应用以出乎用户意料的方式或在未适当通知用户或征得用户同意的情况下，将设备上的数据传输出去。

“移动垃圾软件”政策

公开行为和明确披露信息

所有代码都应兑现对用户的承诺。应用应提供所有已宣传的功能。应用不应使用户感到困惑。

违规行为示例：

- 广告欺诈
- 社交工程

保护用户数据

对个人数据及敏感用户数据的访问、使用、收集和分享应保持透明。对用户数据的使用必须遵守所有相关的用户数据政策（如适用），并采取所有预防措施来保护数据。

违规行为示例：

- 数据收集（请参阅“间谍软件”）
- 受限权限滥用

查看完整的“移动垃圾软件”政策

“设备和网络滥用”政策

我们不允许应用干扰、中断、损害或以未经授权的方式访问用户的设备、其他设备/计算机、服务器、网络、应用编程接口 (API) 或服务，包括但不限于相应设备上的其他应用、任何 Google 服务或授权运营商的网络。

如果应用或第三方代码（例如 SDK）会在运行时加载 JavaScript、Python 或 Lua 等解释型语言（例如未打包到应用软件包中的此类代码），则不得允许可能违反 Google Play 政策的行为。

我们不允许任何代码引入或利用安全漏洞。查看应用安全性改进计划，了解应用开发者需注意的最新安全问题。

查看完整的“设备和网络滥用”政策。

SDK 导致的违规行为示例

- 对于帮助向第三方提供代理服务的应用，该服务必须是其面向用户提供的主要核心功能。
- 应用中的 SDK 会从 Google Play 以外的其他来源下载可执行代码，例如 dex 文件或原生代码。
- 应用中的 SDK 包含具有额外 JavaScript 接口的 WebView，并且该接口会加载不受信任的网络内容（例如 http:// 网址）或从不受信任的来源获取的未经验证的网址（例如，通过不受信任的 intent 获取的网址）。
- 应用中的 SDK 包含用于更新其自身 APK 的代码
- 应用中的 SDK 会通过不安全的连接下载文件，从而导致用户面临安全漏洞的威胁。
- 应用使用的 SDK 包含会从 Google Play 以外的未知来源下载或安装应用的代码。
- 应用中的 SDK 会使用前台服务，但并非在适当的使用情形下。
- 应用中的 SDK 会出于符合政策规定的原因而使用前台服务，但并未在应用的清单进行声明。

“欺骗性行为”政策

我们不允许发布任何试图欺骗用户或协助促成不诚实行为的应用，包括但不限于被判定为功能上无法兑现其承诺的应用。应用必须在其元数据的所有部分中针对自身功能提供准确的声明、说明和相关图片/视频。应用不得试图模仿操作系统或其他应用的功能或警告。对设备设置的任何更改都必须在用户知情并同意的情况下进行，而且必须允许用户撤消。

请参阅完整的“欺骗性行为”政策。

行为透明度

对普通用户而言，应用功能应清楚明了；应用中应不包括任何隐藏的、休眠的或未载明的功能。我们禁止使用可用于规避应用审查的技术。应用可能需要提供额外的详细信息，以确保用户安全、系统完整性和政策遵从性。

SDK 导致的违规行为示例

- 您的应用包含利用技术来规避应用审查的 SDK。

哪些 Google Play 开发者政策通常涉及到 SDK 导致的违规行为？

为帮助您确保应用使用的所有第三方代码都符合 Google Play 开发者计划政策，请参阅以下各项政策全文：

- 用户数据政策
- 敏感信息访问权限和 API
- “设备和网络滥用”政策
- 恶意软件
- 移动垃圾软件
- 家庭内容自行认证广告 SDK 计划
- 广告政策
- 欺骗性行为
- Google Play 开发者计划政策

以上介绍了常见违规问题涉及的一些政策，不过请谨记，不良的 SDK 代码也可能会导致应用违反上文中未提及的其他政策。作为应用开发者，您有责任确保所用 SDK 处理应用数据的方式符合政策，请务必通读并及时全面了解所有政策。

如需了解详情，请访问我们的帮助中心。

恶意软件

我们的恶意软件政策很简单：保护 Android 生态系统（包括 Google Play 商店）和用户设备免遭恶意行为（例如恶意软件攻击）侵扰。秉持这一基本原则，我们积极致力于向用户及其 Android 设备提供安全的 Android 生态系统。

恶意软件是指任何可能给用户、用户数据或设备带来风险的代码。恶意软件包括但不限于潜在有害应用 (PHA)、二进制文件或框架修改，所涵盖的类别包括特洛伊木马、钓鱼式攻击和间谍软件应用等。我们会不断更新并添加新类别。

此政策的要求也适用于您在应用中纳入的任何第三方代码（例如 SDK）。

虽然恶意软件的类型和功能有别，但通常都是为了达成以下某种目的：

- 破坏用户设备的完整性。
- 取得用户设备的控制权。
- 实现远程控制操作，以便攻击者访问、使用或以其他方式利用受感染的设备。
- 在未充分告知用户并征得同意的情况下，擅自将个人数据或凭据从设备上传输出去。
- 通过受感染的设备传播垃圾内容或命令，意在影响其他设备或网络。
- 欺骗用户。

应用、二进制文件或框架修改具有潜在危害性，因此即便这些内容本身无意造成危害，也可能会产生恶意行为。这是因为应用、二进制文件或框架修改内容的运作方式可能会因诸多可变因素而发生变化。因此，对某个 Android 设备有害的内容对其他 Android 设备可能完全不会构成威胁。例如，对于搭载 Android 最新版本的设备而言，使用已弃用的 API 进行恶意行为的有害应用不会产生任何影响，但对于仍搭载 Android 早期版本的设备，这类应用可能会造成风险。如果应用、二进制文件或框架修改会给部分或所有 Android 设备和用户明确带来风险，就会被标记为恶意软件或 PHA。

通过下方的恶意软件类别，我们不仅希望传达我们的基本理念，即让用户了解自己设备遭利用的情形，同时也要推广安全的生态系统，以推动稳健的创新发展并打造值得信赖的用户体验。

有关详情，请访问 Google Play 保护机制 。

后门程序

此类代码允许在某个设备上执行不需要的、可能有害的远程控制操作。

如果自动执行，这些操作包含的行为可能会导致应用、二进制文件或框架修改变成其他某种恶意软件。一般来说，后门程序描述了可能有害的操作在设备上的发生方式，因此不完全等同于结算欺诈或商业间谍软件等类别。因此，在某些情况下，Google Play 保护机制会将部分后门程序视为漏洞。

帐单欺诈

此类代码会通过蓄意欺骗的方式自动向用户收费。

手机帐单欺诈分为短信欺诈、电话欺诈和收费欺诈。

短信欺诈
此类代码会在未经用户同意的情况下发送付费短信，或者试图通过隐藏披露协议或移动运营商向用户发送的收费或订阅确认通知短信来掩盖其短信活动，进而达到向用户收取费用的目的。

有些代码尽管从技术层面披露了自身的短信发送行为，但是会引入其他可能构成短信欺诈的行为。例如，对用户隐藏披露协议的部分内容，使其无法阅读；有条件地隐藏移动运营商向用户发送的收费或订阅确认通知短信。

电话欺诈
此类代码会在未经用户同意的情况下通过拨打付费电话号码向用户收取费用。

收费欺诈
此类代码会诱骗用户通过手机帐单代扣方式订阅或购买内容。

收费欺诈包括除付费短信和付费电话欺诈之外所有类型的帐单欺诈。相关示例包括与运营商直接代扣、无线接入点 (WAP) 和手机话费转移相关的欺诈。WAP 欺诈是最常见的收费欺诈之一。WAP 欺诈的形式包括诱骗用户在悄声加载的透明 WebView 上点击一个按钮。用户执行该操作后，就会触发一项周期性订阅，通常此类订阅的确认短信或电子邮件会被劫持，从而导致用户无法注意到相关的财务交易。

跟踪软件

出于监控目的，从设备中收集个人数据或敏感用户数据，并将相应数据传输至第三方（企业或其他个人）的代码。

根据用户数据政策 规定，应用必须提供适当的醒目披露声明并征得用户同意。

关于监控应用的准则

专为监控其他个人（例如父母监管自己的孩子或企业管理者监控员工）而设计和推广且完全符合下述要求的应用，才是可接受的监控应用。此类应用不得用于跟踪任何其他人（例如，配偶），无论跟踪目标是否知情或许可，也无论应用是否显示常驻通知，都是如此。这些应用必须在其清单文件中使用 IsMonitoringTool 元数据标记以适当方式宣称自身为监控应用。

监控应用必须符合以下要求：

- 应用不得标明是用于暗中监控或秘密监视用途。
- 应用不得隐藏或掩盖跟踪行为，或试图误导用户来隐瞒这类功能的真正用途。
- 应用在运行期间必须始终向用户显示常驻通知，并呈现可清楚识别该应用的独特图标。
- 应用必须在 Google Play 商店说明中披露监控或跟踪功能。
- Google Play 上的应用及其应用详情不得提供任何途径来激活或使用违反上述条款的功能（例如链接到在 Google Play 以外托管的不符合规定的 APK）。
- 应用必须遵守所有适用的法律规定。您须自行负责确定应用在目标语言区域的合法性。

如需了解详情，请参阅帮助中心的使用 IsMonitoringTool 标志　一文。

拒绝服务攻击 (DoS)

此类代码会在用户不知情的情况下对其他系统和资源执行拒绝服务攻击 (DoS)，或者构成分布式 DoS 攻击的一环。

例如，它们可以通过发送大量 HTTP 请求使远程服务器上产生过多的负载，从而达到攻击目的。

恶意下载程序

此类代码本身没有潜在危害，但会下载其他 PHA。

如果某个应用符合以下情况，它就可能是恶意下载程序：

- 有依据表明它是为了传播 PHA 而开发的，并且已经下载了 PHA，或者包含可下载并安装应用的代码；或者
- 在监测量不低于 500 次应用下载的情况下，检测到它下载的应用中至少有 5% 是 PHA（检测到 25 次 PHA 下载）。

对于主流浏览器和文件共享应用，只要满足以下条件，便不属于恶意下载程序：

- 它们不会在无用户交互的情况下触发下载；并且
- 所有 PHA 下载都是在用户同意的情况下启动的。

非 Android 威胁

此类代码包含非 Android 威胁。

使用此类代码的应用不会对 Android 用户或设备造成危害，但包含可能对其他平台有害的组件。

网上诱骗

此类代码假装来自可信来源，请求获取用户的身份验证凭据或结算信息，并向第三方发送数据。此类别还包括在用户凭据传输过程中拦截传输行为的代码。

网上诱骗常见的攻击目标包括银行凭据、信用卡号，以及社交网络和游戏的在线帐号凭据。

滥用超出规定的权限的行为

此类代码通过以下方式破坏系统完整性：破坏应用沙盒、获取超出规定的权限，或者更改或禁止核心安全相关功能的访问权限。

例如：

- 应用违反 Android 权限模型，或从其他应用窃取凭据（例如 OAuth 令牌）。
- 应用滥用防卸载或防关停功能。
- 应用停用 SELinux。

未经用户同意取得设备 root 权限的提权应用会被划分为获取 root 权限的应用。

勒索软件

此类代码会对设备或设备上的数据施加一定程度或严密的控制，用户必须付款或执行某项操作才能解除控制。

某些勒索软件会加密设备上的数据，要求用户付款后才会解密数据，并且（或者）会利用设备管理员功能，让普通用户无法移除这些数据。例如：

- 锁定设备，使用户无法访问，并要求用户花钱赎回控制权。
- 加密设备上的数据，以解密数据为由要求用户付款。
- 利用设备政策管理器功能，阻止用户移除数据。

如果使用设备分发的代码的主要目的是辅助设备管理，则我们可能会不将这类代码视为勒索软件，但前提是这类代码全面满足安全锁定和管理要求，并充分满足用户告知和意见征求要求。

启用 root 权限

此类代码会启用设备的 root 权限。

启用 root 权限的代码有非恶意和恶意之分。例如，要启用 root 权限的非恶意应用会提前告知用户它们将启用设备的 root 权限，并且不会执行属于其他 PHA 类别的其他潜在危害性操作。

然而，要启用 root 权限的恶意应用不会告知用户它们将启用设备的 root 权限，或者尽管会提前告知用户启用 root 权限的行为，但是还会执行属于其他 PHA 类别的其他操作。

垃圾邮件

此类代码会向用户的联系人发送垃圾消息，或将设备用作垃圾邮件中继。

间谍软件

间谍软件是指会收集、泄露或分享与符合政策的功能无关的用户数据或设备数据的恶意应用、代码或行为。

可视为对用户执行间谍活动或者在没有适当通知用户或征得用户同意的情况下泄露数据的恶意代码或行为也被视为间谍软件。

例如，间谍软件违规行为包括但不限于：

- 录音或或对通话录音
- 窃取应用数据
- 具有恶意第三方代码（例如 SDK）的应用以出乎用户意料的方式或在未适当通知用户或征得用户同意的情况下，将设备上的个人数据传输出去。

所有应用还必须遵守所有 Google Play 开发者计划政策，包括有关用户数据和设备数据的政策，例如“移动垃圾软件”政策、“用户数据”政策、“敏感信息访问权限和 API”政策 以及 SDK 要求。

特洛伊木马

此类代码看似没有问题（例如声称自己只是一款游戏的游戏），但会针对用户执行用户不想要的操作。

这种类别的代码通常会与其他 PHA 类别的代码混合在一起。特洛伊木马由一个看似无害的组件和一个隐藏的有害组件构成。例如，某游戏在用户不知情的情况下，在后台从用户的设备发送付费短信。

关于不常见应用的说明

对于新的和罕见的应用，如果 Google Play 保护机制掌握的信息较少，无法明确判定是否安全，则可能会将其分类为不常见的应用。这并非意味着这类应用一定有害，但如果未经进一步审核，也不能明确确定其一定安全。

关于后门程序类别的说明

后门程序恶意软件类别的分类取决于代码行为。将代码归类为后门程序的必要条件是：如果自动执行，这种代码所实现的行为会导致其变成其他某种恶意软件。例如，如果某应用允许动态加载代码，并且动态加载的代码会提取文本消息，则该应用会被归类为后门程序恶意软件。

但是，如果某应用允许执行任意代码，而且我们没有理由认为该代码执行行为是为了达成恶意目的，则该应用会被视为存在漏洞（不会被视为后门程序恶意软件），我们会要求开发者进行修补。

伪装软件

一种利用多种规避技术向用户提供不一致或虚假功能的应用。此类应用会伪装成合法的应用或游戏，使其在应用商店中看似无害，并利用诸如混淆、动态代码加载或伪装真实内容等技术来显示恶意内容。

Maskware 与其他 PHA 类别（特别是特洛伊木马）相似，但主要区别在于会采用各种技术来混淆恶意活动。

假冒行为

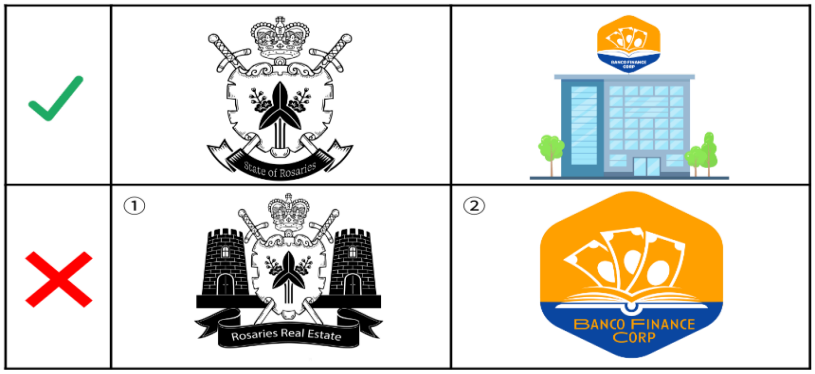
我们不允许任何应用通过假冒他人（例如其他开发者、公司、实体）或其他应用来误导用户。请勿在应用与某人并无关联或未获其授权的情况下，暗示您的应用与其相关或已获得其授权。请注意避免使用可能会使用户误以为您的应用与其他人或其他应用存在关联的应用图标、说明、名称或应用内元素。

下面是常见违规行为的一些示例：

- 开发者不实地暗示与其他公司/开发者/实体/组织存在关系。

① 此应用中所列的开发者名称暗示此应用与 Google 之间有官方关系（实际上子虚乌有）。

- 应用的图标和名称不实地暗示与其他公司/开发者/实体/组织存在关系。



① 应用使用国徽，让用户误以为此应用与政府有关联。
② 应用抄袭某商业实体的徽标，不实地暗示应用是该实体的官方应用。

- 应用的名称和图标与现有产品或服务的名称和图标十分相似，可能会误导用户。

① 应用在其应用图标中使用某个热门的加密货币网站的徽标，暗示它是官方网站。
② 应用在其应用图标中抄袭某个著名电视节目的人物及名称，让用户误以为它与该电视节目有关。

- 应用不实声称是某知名实体的官方应用。举例来说，在未获得必要许可或权利的情况下，应用不得使用诸如“贾斯汀·比伯官方应用”之类的标题。
- 应用违反 Android 品牌推广指南 。

对于与“假冒”政策有关的常见问题解答，请参阅这篇帮助中心文章。

移动垃圾软件

在 Google，我们坚信以用户为中心，其他一切自然水到渠成。在软件准则和垃圾软件政策中，我们针对可提供良好用户体验的软件提供了一般性建议。此项政策以 Google 垃圾软件政策为基础，概述了 Android 生态系统和 Google Play 商店的相关准则。违反这些准则的软件可能会给用户体验造成负面影响，我们将采取措施保护用户免遭此类软件的侵扰。

正如垃圾软件政策中所述，我们发现大多数垃圾软件都具有一个或多个相同的基本特征：

- 具有欺骗性，承诺其无法实现的价值主张。
- 诱骗用户进行安装，或搭载在用户安装的其他程序上。
- 不向用户告知其所有主要功能和重要功能。
- 以非预期方式影响用户的系统。
- 在用户不知情的情况下收集或传输隐私信息。
- 在未经安全处理的情况下收集或传输隐私信息（例如，通过 HTTPS 传输）。
- 与其他软件捆绑在一起，但并未将这一情况告知用户。

在移动设备上，软件是采用应用、二进制文件、框架修改等形式的代码。为了防止软件对软件生态系统产生有害影响或破坏用户体验，我们将对违反这些准则的代码采取相应措施。

以下是我们根据垃圾软件政策制定的政策，其适用范围扩展到了移动软件。通过该政策，我们将继续优化此移动垃圾软件政策，以应对新型滥用行为。

公开行为和明确披露信息

所有代码都应兑现对用户的承诺。应用应提供所有已宣传的功能。应用不应使用户感到困惑。

- 应用应明确功能和目的。
- 清晰明确地向用户说明应用将进行哪些系统更改。允许用户查看和核准所有重要的安装选项和更改。
- 软件不得向用户谎报用户设备的状态，例如，声称系统处于重大安全风险状态或已感染病毒。
- 请勿利用旨在增加广告流量和/或转化次数的无效活动。
- 我们不允许任何应用通过假冒他人（例如其他开发者、公司、实体）或其他应用来误导用户。请勿在应用不与某人相关或未获其授权的情况下，暗示您的应用与其相关或已获得其授权。

违规情况示例：

- 广告欺诈
- 社会工程学

保护用户数据和隐私

对个人数据及敏感用户数据的访问、使用、收集和分享应保持透明。对用户数据的使用必须遵守所有相关的用户数据政策（如适用），并且必须采取所有必要的预防措施来保护数据。

所有应用都必须遵守所有 Google Play 开发者计划政策，包括用户和设备数据政策，例如“用户数据”政策、“敏感信息访问权限和 API”政策、“间谍软件”政策以及 SDK 要求。

- 不得要求或诱骗用户关闭设备安全防护功能，例如 Google Play 保护机制。例如，您不得以关闭 Google Play 保护机制为条件向用户提供额外的应用功能或奖励。

不得破坏移动体验。

用户体验应简单明了、易于理解，并且应以用户做出的明确选择为基础。应向用户展示明确的价值主张，而且不得破坏其所宣传的或预期的用户体验。

- 不得以意想不到的方式向用户展示广告，包括损害或干扰设备功能的可用性，或在广告无法轻松关闭或未征得用户充分同意和未明确提供方的情况下，在触发广告的应用之外展示广告。
- 应用不得干扰其他应用或设备的易用性。
- 当应用在适当情况下要进行卸载操作时应明确告知用户。
- 移动软件不得模仿设备操作系统或其他应用的提示。不得禁止其他应用或操作系统向用户发送提醒，尤其是那些提醒用户操作系统更改的提醒。

违规情况示例：

- 干扰性广告
- 未经授权使用或模仿系统功能

恶意下载程序

代码本身不属于垃圾软件，但会下载其他移动垃圾软件 (MUwS)。

如果代码符合以下情况，它就可能是恶意下载程序：

- 有依据表明代码是为了传播 MUwS 而开发，并且已经下载了 MUwS，或者包含可下载并安装应用的代码；或者
- 在监测量不低于 500 次应用下载的情况下，检测到它下载的应用中至少有 5% 是 MUwS（检测到 25 次 MUwS 下载）。

对于主流浏览器和文件共享应用，只要满足以下条件，便不属于恶意下载程序：

- 它们不会在无用户交互的情况下触发下载；并且
- 所有软件下载都是在用户同意的情况下启动的。

广告欺诈

严禁广告欺诈。广告欺诈是指以欺骗广告联盟相信流量源自用户的真实兴趣为目的而生成的广告互动，广告欺诈是一种无效流量。广告欺诈可能是开发者以违禁方式实施广告的副产物。这些违禁方式包括展示隐藏广告，自动点击广告、更改或修改信息以及以其他方式利用非人为操作（蜘蛛程序、自动程序等），或专为产生无效广告流量而设计的人为活动。无效流量和广告欺诈行为会损害广告主、开发者和用户，并且从长期角度导致移动广告生态系统失去信任。

下面是常见违规行为的一些示例：

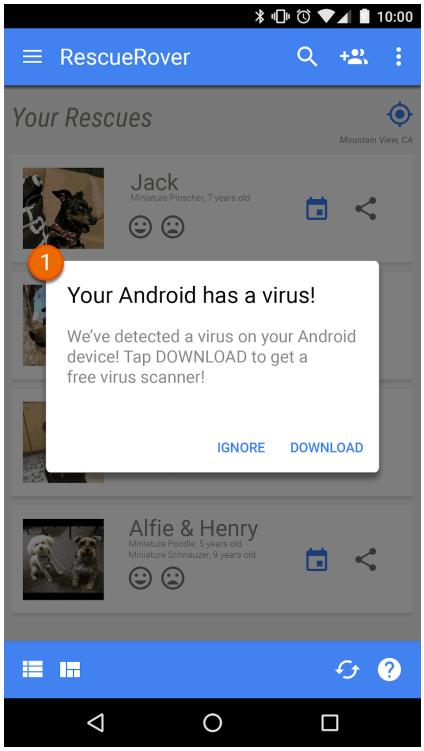
- 应用呈现用户无法看见的广告。
- 应用会在用户无意的情况下自动生成广告点击，或产生同等的网络流量以欺骗性地生成点击数。
- 应用发送虚假安装归属点击，以通过并非在发送者网络执行的安装来获得收入。
- 应用在用户未进入应用界面时显示广告。
- 应用对广告资源进行虚假陈述。例如，当在 Android 设备上运行时，应用向广告联盟通告其在 iOS 设备上运行；应用掩饰用来获利的应用包名称。

未经授权使用或模仿系统功能

我们不允许任何应用或广告模仿或干扰系统功能（如通知或警告）。系统级通知仅限用于应用的基本功能，例如，航班应用可通知用户特价机票信息，或者游戏应用可通知用户游戏内的促销信息。

下面是常见违规行为的一些示例：

- 通过系统通知或提醒显示的应用或广告：



① 此应用中显示的系统通知被用于投放广告。

如需了解涉及广告的其他示例，请参阅广告政策。

社会工程学

我们不允许任何应用通过冒充其他应用，企图诱骗用户执行他们实际上是想在受信任的应用中执行的操作。

获利和广告

Google Play 支持各种变现策略（其中包括付费应用分发、应用内商品、订阅和广告变现模式），致力于让开发者和用户从中受益。为确保提供最佳用户体验，请务必遵守以下政策。

付款

1. 如果要通过 Google Play 提供付费下载应用，开发者必须使用 Google Play 结算系统作为这类交易的付款方式。
2. 通过 Play 分发的应用如果针对应用内功能或服务（包括任何应用功能、数字内容或商品；统称为“应用内购商品”）要求或接受付款，必须使用 Google Play 结算系统进行这类交易，但适用第 3 条、第 8 条或第 9 条的情况除外。

   某些应用功能或服务需要使用 Google Play 结算系统进行收费，具体示例包括但不限于以下应用内购商品：

   - 商品（例如虚拟货币、额外生命、额外游戏时间、附加道具、角色和头像）；
   - 订阅服务（例如健身、游戏、约会交友、教育、音乐、视频、服务升级和其他内容订阅服务）；
   - 应用功能或内容（例如应用的无广告版本，或免费版本中不提供的新功能）；
   - 云软件和服务（例如数据存储服务、企业办公软件和财务管理软件）。

3. 在以下情况下，不得使用 Google Play 结算系统：
   a. 付款的主要目的为：
      - 购买或租借实体商品（例如杂货、服装、家用器具、电子产品）；
      - 购买实际服务（例如交通服务、清洁服务、机票、健身房会员、食品外卖、现场活动的门票）；或
      - 信用卡还款或生活缴费（例如有线电视服务和电信服务）；

   b. 付款包括点对点付款、在线竞价和免税捐款；
   c. 付款是为了购买为在线赌博提供便利的内容或服务，具体如“现金赌博、游戏和竞赛”政策的赌博应用部分中所述；
   d. 付款涉及 Google 付款中心内容政策 认为不可接受的任何商品类别。

   注意：在某些市场，我们针对销售实体商品和/或服务的应用提供 Google Pay 服务。如需了解详情，请访问我们的 Google Pay 开发者 页面。

4. 除第 3 条、第 8 条和第 9 条所述的情况外，应用不得将用户引导至 Google Play 结算系统以外的其他付款方式。这项规定禁止的行为包括但不限于通过以下方式将用户引导至其他付款方式：
   - Google Play 上的应用商品详情；
   - 与可购买内容相关的应用内宣传广告；
   - 应用内 WebView、按钮、链接、消息、广告或其他号召性用语；以及
   - 应用内界面流程（包括账号创建或注册流程），在这些流程中将用户从应用引导至 Google Play 结算系统以外的付款方式。

5. 为某款应用或游戏购买的应用内虚拟货币只能在该应用或游戏内使用。
6. 开发者必须清楚准确地向用户提供其应用或所售的任何应用内功能或订阅服务的条款和定价。应用内价格必须与面向用户的 Play 结算界面中显示的价格一致。在 Google Play 上，如果您在商品说明中提到的应用内功能可能需要支付特定或额外的费用才能使用，则您必须在应用详情中明确告知用户此类功能需要付费才能使用。
7. 如果应用和游戏提供可让用户在购物时获得随机虚拟奖品的机制（包括但不限于“战利品箱”），则必须在用户购买前并且是在即将购买前及时明确披露获得这类奖品的几率。

8. 除非第 3 条所述的情况适用，否则通过 Play 分发的应用如果针对应用内购商品要求或接受这些国家/地区的用户付款，则这类应用的开发者在针对每个具体计划分别填妥结算声明表单并同意其中包含的附加条款和计划要求后，可同时向用户提供应用内备选结算系统以及 Google Play 结算系统来用于进行这类交易。
9. 通过 Play 分发应用的开发者可将欧洲经济区 (EEA) 的用户引导至应用之外进行一些操作，包括通过这种方式来推广应用内数字功能和服务的优惠活动。开发者若想将欧洲经济区 (EEA) 的用户引导至应用之外进行操作，必须先填妥该计划的声明表单，并同意其中包含的附加条款和计划要求。

注意：如需查看有关此政策的时间安排和常见问题解答，请访问我们的帮助中心。

广告

为了维持优质的体验，我们会考虑广告的内容、受众群体、用户体验、行为，以及安全性和隐私保护机制。我们将广告和相关优惠视为应用的组成部分，因此它们也必须遵循所有其他 Google Play 政策。如果您通过 Google Play 上某款面向儿童的应用变现，我们针对广告还有额外的要求。

您还可以在此处详细了解我们的“应用宣传”政策和“商品详情”政策，包括我们如何处理欺骗性宣传行为。

广告内容

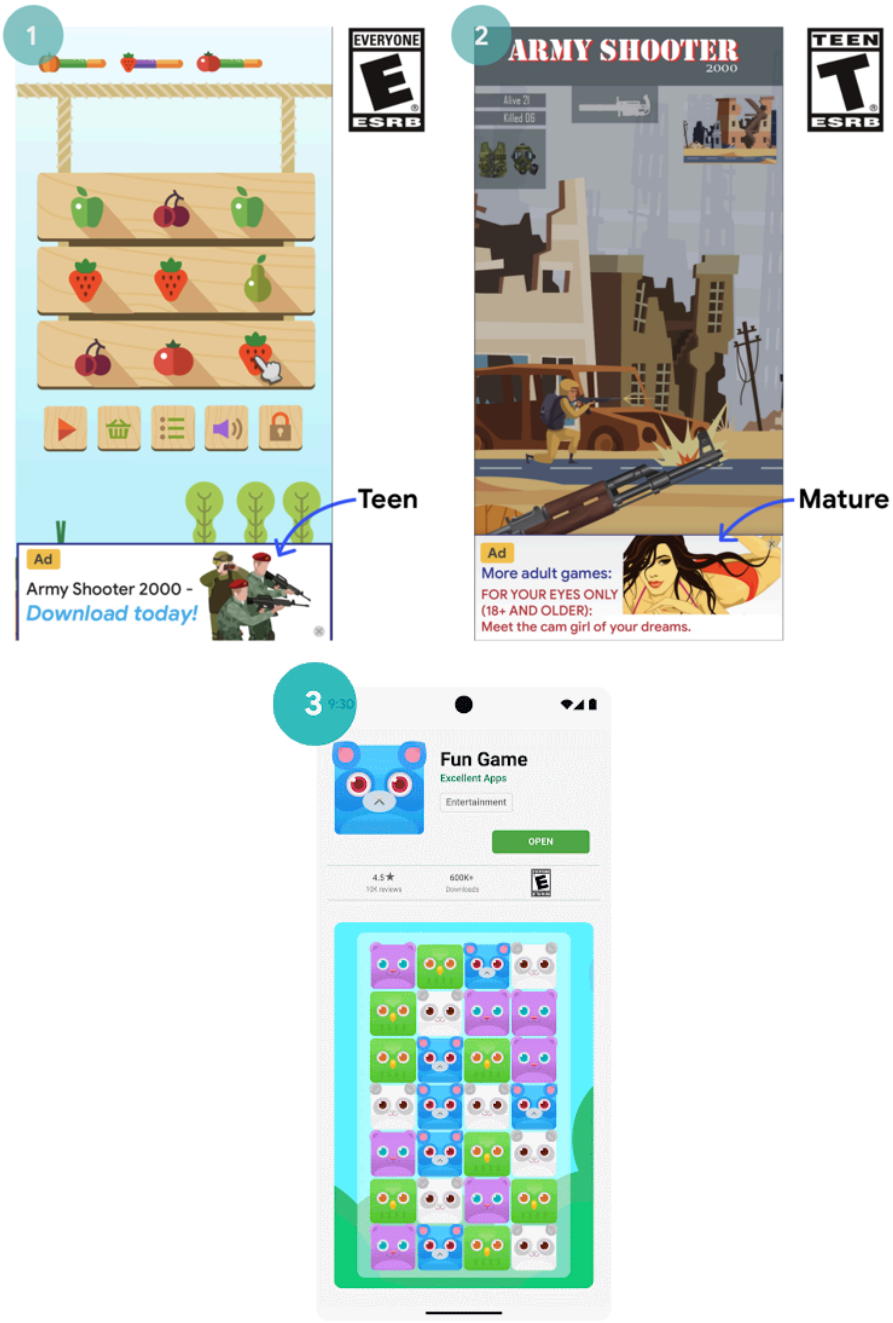
广告和相关优惠属于应用的组成部分，必须遵循我们的受限内容政策。如果您的应用是赌博应用，则还需要遵循额外的相关要求。

不恰当的广告

应用中展示的广告及其相关优惠（例如，广告宣传下载其他应用）必须符合应用的内容分级 ，即使内容本身在其他方面符合我们的政策也是如此。

下面是常见违规行为的一些示例：

- 广告与应用的内容分级不符



① 此广告的目标群体是青少年，不符合应用的内容分级（所有人）
② 此广告的目标群体是成人，不符合应用的内容分级（青少年）
③ 广告的优惠（宣传下载成人应用）不符合展示该广告的游戏应用的内容分级（所有人）

家庭政策中“广告”部分的相关要求

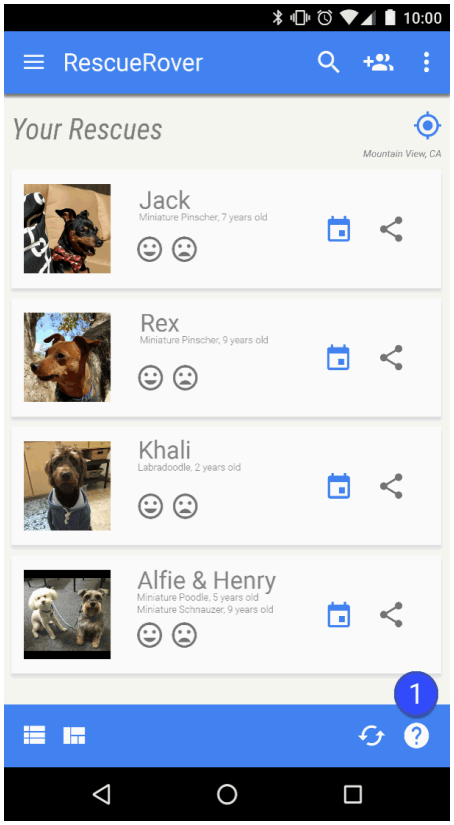
如果您要通过 Google Play 上某款面向儿童的应用变现，则该应用必须遵循家庭政策中“广告和变现”部分的相关要求。

欺骗性广告

广告不得模仿或假冒任何应用功能界面，例如操作系统中的通知或警告元素。您必须明确告知用户，每个广告将在哪个应用中投放。

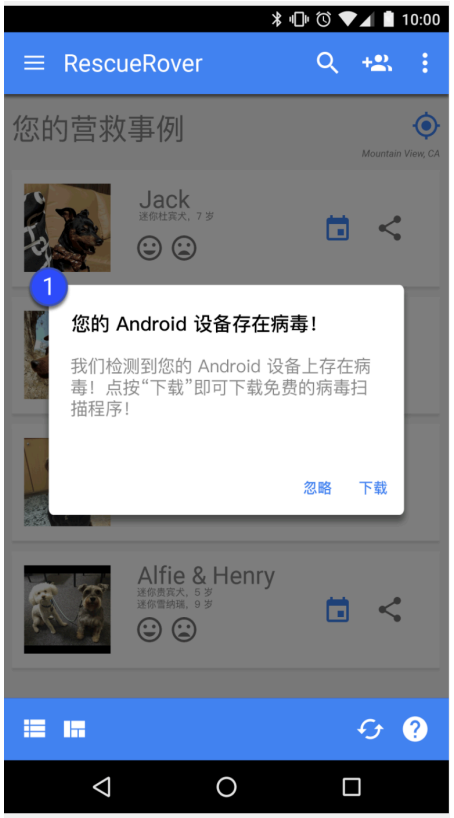
下面是常见违规行为的一些示例：

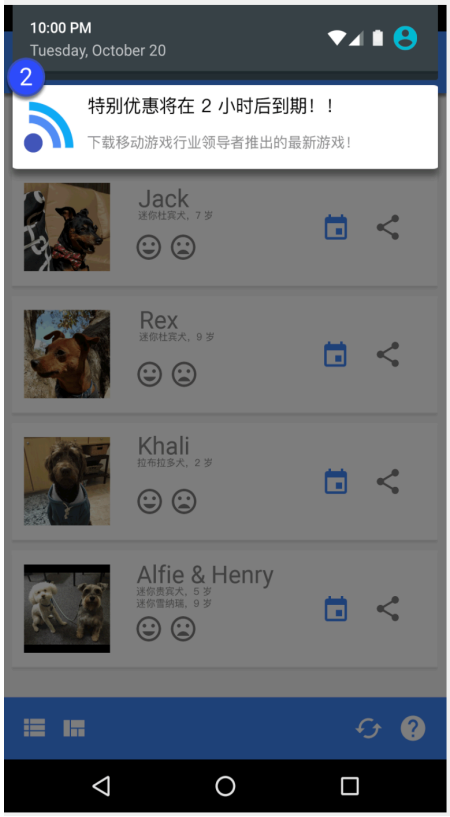
- 模仿应用界面的广告：



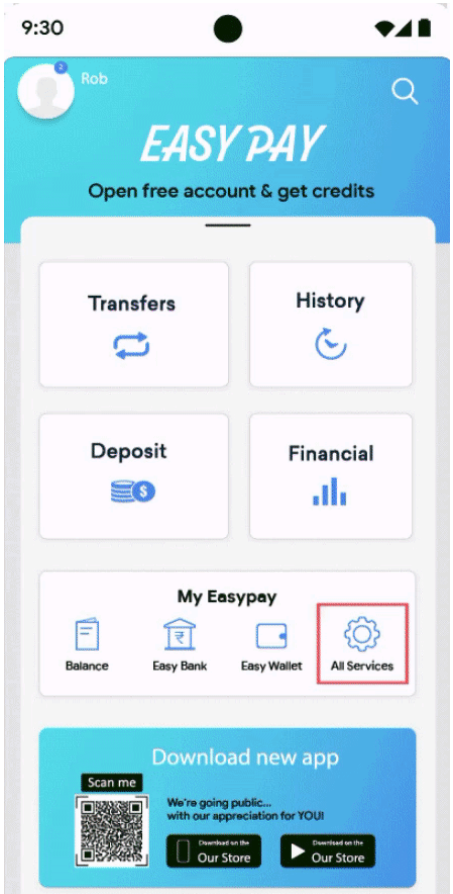
① 此应用中的问号图标是一个广告，可将用户引导至外部着陆页。

- 模仿系统通知的广告：





① ② 上方示例展示了模仿各种系统通知的广告。



① 上方示例展示的功能区域模仿其他功能，但只会将用户引导至一个或多个广告。

干扰性广告

干扰性广告是指以出人意料的方式向用户展示的广告，此类广告可能会导致意外点击，或影响/干扰设备功能的使用。

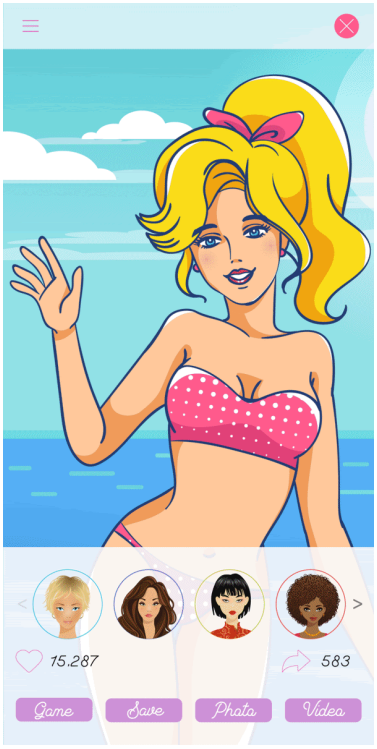
您的应用不得强制要求用户必须点击广告或提交个人信息以用于广告宣传，然后才能使用应用的完整功能。广告只能展示在投放广告的应用内，且不得干扰其他应用、广告或设备（包括系统或设备按钮和端口）的运作。这类广告包括重叠式广告、配套功能和微件化的广告单元。如果您的应用会展示广告或其他干扰正常使用过程的广告，您必须让用户能够轻松将其关闭且不会因此受到任何不利影响。

下面是常见违规行为的一些示例：

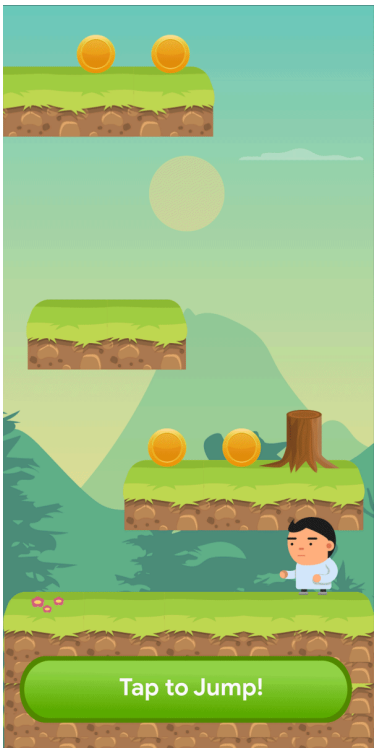
- 广告占据整个屏幕或干扰用户正常使用，且未提供明确的关闭方式：

① 此广告未提供关闭按钮。

- 广告通过以下方式强制用户点击：使用虚假关闭按钮，或突然出现在应用中通常供用户点按访问其他功能的区域：

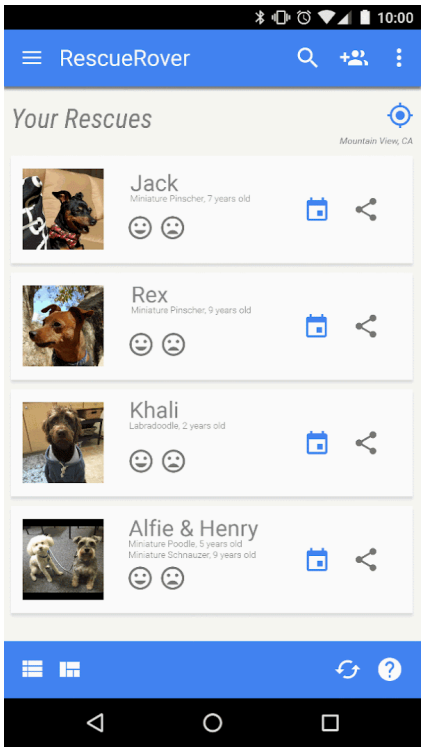


① 此广告使用虚假关闭按钮。



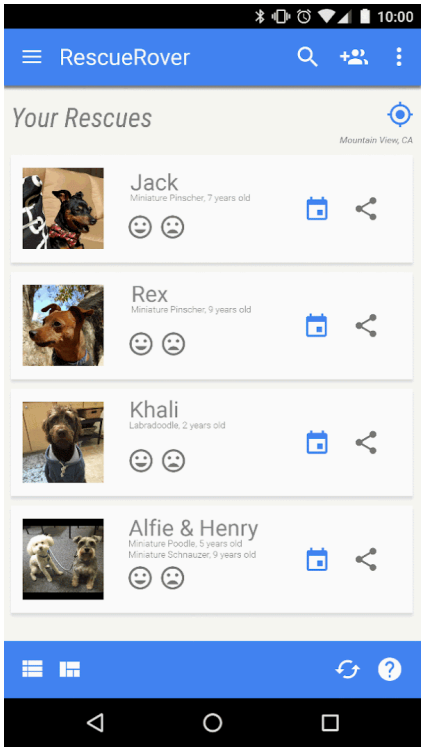
② 此广告突然出现在用户通常点按来访问应用内功能的区域。

- 在投放相应广告的应用外展示这些广告：



① 用户从该应用前往主屏幕时，主屏幕上突然显示广告。

- 广告通过主屏幕按钮或其他专用于退出应用的功能触发：



① 用户尝试退出应用并前往主屏幕，但预期的操作流程却被广告打断。

优质的广告体验

开发者必须遵守以下广告准则，以确保用户在使用 Google Play 应用时获得出色的体验。不得以下列非预期的方式向用户展示您的广告：

- 不允许以非预期的方式（通常是在用户选择做其他事时）展示任何格式（视频、GIF、静态等）的全屏插页式广告。
  - 不允许在游戏过程中某个关卡开始时或在某个内容片段开始时展示广告。

- 不允许在应用的加载屏幕（启动画面）显示之前展示全屏插页式视频广告。
- 不允许展示 15 秒后无法关闭的任何格式的全屏插页式广告。选择启用的全屏插页式广告或不会干扰用户操作（例如，在游戏应用中的得分屏幕后展示）的全屏插页式广告可以持续展示 15 秒以上。

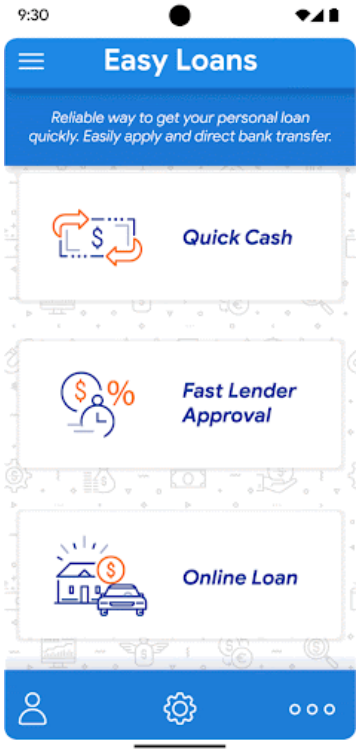
此政策不适用于用户明确选择启用的激励广告（例如，开发者明确提供给用户观看，用来换取解锁特定游戏功能或内容片段等奖励的广告）。此政策也不适用于不会干扰用户正常使用应用或玩游戏的变现内容和广告内容（例如，包含集成广告的视频内容、非全屏横幅广告）。

这些准则是参照优质广告标准 - 移动应用体验　准则。如需详细了解优质广告标准，请参阅 Coalition for Better Ads　网站。

下面是常见违规行为的一些示例：

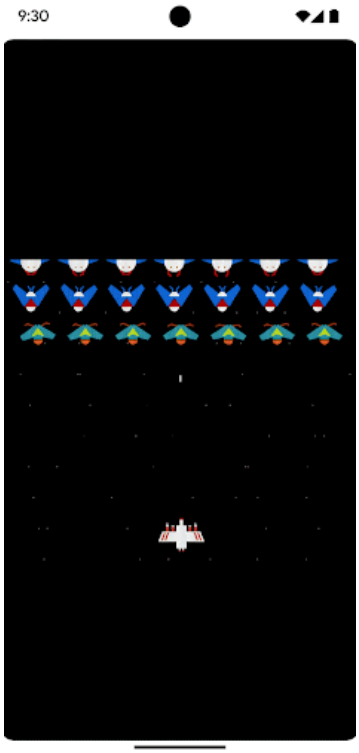
- 广告在游戏过程中或某个内容片段开始时以非预期的方式展示（例如，在用户点击某个按钮之后，以及点击按钮后的预期操作生效之前）。这些广告对于用户来说出乎意料，因为用户原本希望开始玩游戏或查看相应内容。

① 静态广告在游戏过程中的某个关卡开始时以非预期的方式展示。



② 视频广告在某个内容片段开始时以非预期的方式展示。

- 全屏广告在游戏过程中展示，且在 15 秒后无法关闭。



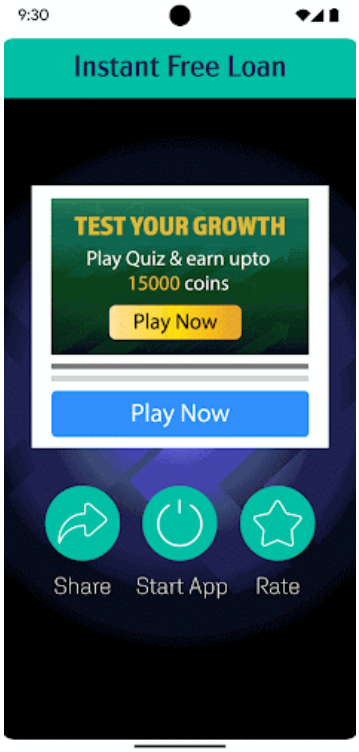
① 插页式广告在游戏过程中展示，且未向用户提供在 15 秒内跳过广告的选项。

以投放广告为目的

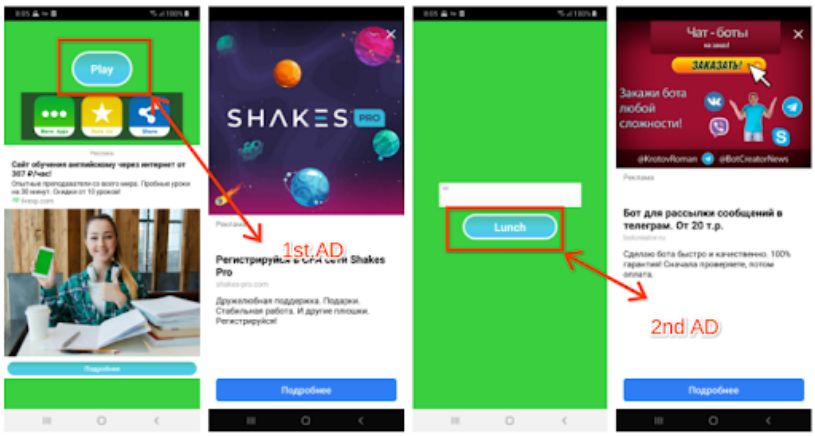
我们不允许任何应用重复展示会干扰用户与应用互动和执行应用内任务的插页式广告。

下面是常见违规行为的一些示例：

- 在用户执行操作（包括但不限于点击、滑动等）后连续展示插页式广告的应用。



① 首个应用内页面具有多个可与之互动的按钮。当用户点击**启动应用**来使用应用时，系统弹出一个插页式广告。用户在关闭该广告后返回应用，并点击**服务**，希望开始使用相应服务，但系统展示了另一个插页式广告。



② 在首个页面中，系统引导用户点击**开始游戏**，因为这是应用页面上唯一一个可用的按钮。当用户点击该按钮后，系统展示了一个插页式广告。用户在关闭该广告后点击**启动**，因为这是页面上唯一一个可互动的按钮，结果系统弹出了另一个插页式广告。

利用锁屏功能获利

除非应用的用途就是锁屏，否则应用不得提供通过设备锁定屏幕获利的广告或功能。

广告欺诈

我们严禁广告欺诈行为。如需了解详情，请参阅我们的广告欺诈政策。

出于广告目的使用位置数据

如果应用将基于权限获取的设备位置数据额外用于广告投放，则必须遵守个人信息和敏感信息政策，同时还必须满足以下要求：

- 如果您出于广告目的而使用或收集基于权限获取的设备位置数据，则必须明确告知用户，并且在我们硬性要求提供的应用隐私权政策中明确说明，其中应添加指向所有涉及位置数据使用的相关广告网络隐私

权政策的链接。

- 根据位置权限的相关要求，您只能出于实现应用内现有功能或服务的目的而请求设备位置权限，而不得纯粹出于广告目的请求该权限。

Android 广告 ID 的使用

Google Play 服务 4.0 版中引入了新的 API 和 ID，可供广告和分析服务提供商使用。此 ID 的使用条款如下。

- **用途**：Android 广告标识符 (AAID) 只能用于投放广告和进行用户分析。每次使用该 ID 时，都必须确认“选择停用针对用户兴趣投放广告”或“选择停用广告个性化功能”设置的状态。
- **与个人身份信息或其他标识符的关联**。
  - 广告用途：不得出于任何广告目的将该广告标识符与永久性设备标识符（例如 SSAID、MAC 地址、IMEI 等）相关联。只有在获得用户明确许可的情况下，才能将该广告标识符与个人身份信息相关联。
  - 分析用途：不得出于任何分析目的将广告标识符与个人身份信息或任何永久性设备标识符（例如 SSAID、MAC 地址、IMEI 等）相关联。如需了解永久性设备标识符方面的其他指南，请参阅用户数据政策 。
- **尊重用户的选择**。
  - 广告标识符重置后，在未获得用户明确许可的情况下，不得将新的广告标识符与先前的广告标识符或由先前的广告标识符所衍生的数据相关联。
  - 此外，您必须遵从用户的“选择停用针对用户兴趣投放广告”或“选择停用广告个性化功能”设置。如果用户已启用此设置，您不得出于广告目的使用该广告标识符创建用户个人资料，也不得使用该广告标识符向用户投放个性化广告。允许的活动包括：内容相关广告投放、频次上限、转化跟踪、生成报表，以及安全性和欺诈检测。
  - 在操作系统版本较高的设备上，当用户删除 Android 广告标识符时，该标识符将被移除。届时，任何尝试获取该标识符的操作都会收到一串零。不得将没有广告标识符的设备关联到与先前的广告标识符关联的数据或由先前的广告标识符所衍生的数据。
- **向用户明确披露相关信息**。您必须通过符合法律规范的隐私权声明向用户披露对广告标识符的收集和使用行为，以及对于这些条款的遵守义务。如需详细了解我们的隐私保护标准，请参阅我们的用户数据政策。
- **遵守使用条款**。使用该广告标识符时，必须遵守《Google Play 开发者计划政策》；如果因业务所需而与任何第三方分享该广告标识符，对方也必须遵守该政策。所有上传或发布到 Google Play 的应用若要投放广告，都必须使用该广告 ID（如果设备提供的话），而非任何其他设备标识符。

如需了解详情，请参阅我们的用户数据政策。

订阅

作为开发者，您在介绍应用内的订阅服务或内容时不得提供任何会误导用户的信息。您应在所有应用内促销活动或启动画面中清晰传达产品/服务信息，这一点至关重要。我们不允许发布会为用户带来欺骗性或操纵式购买体验（包括应用内购买或订阅）的应用。

您必须清晰明确地传达产品/服务信息。这包括明确说明您的订阅方案条款、订阅费用、结算周期频率以及用户是否必须订阅才能使用该应用。对于此类信息，应让用户无需执行任何额外操作即可查看到。

订阅产品必须能在整个订阅期内向用户提供持续性或周期性的价值，并且不得用于向用户提供本质上属于一次性福利的内容（例如，提供一次性应用内抵用金/代币或一次性游戏强化道具的 SKU）。您的订阅产品可以提供奖励或推广奖金，但这些激励必须作为在整个订阅期内向用户提供的持续性或周期性价值的补充内容。不提供持续性和周期性价值的产品必须设置为应用内商品而非订阅产品。

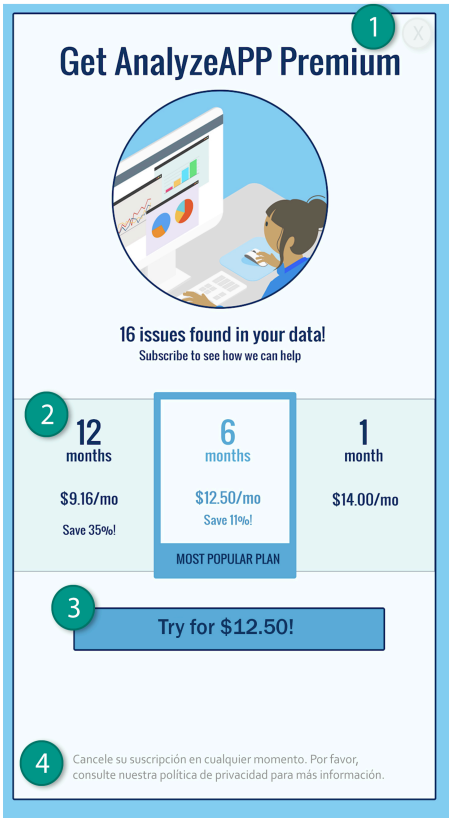
您不得伪装或虚假描述一次性福利，让用户将其误认为是订阅产品。这包括在用户购买订阅产品后，将其修改为一次性产品（例如，取消、废弃或最大限度降低提供的周期性价值）。

下面是常见违规行为的一些示例：

- 提供按月订阅，但没有向用户说明该订阅会每月自动续订和收费。

- 按年订阅方案醒目地显示以每月费用为单位的价格。
- 订阅价格和条款未完全本地化。
- 应用内促销活动未明确说明用户可以在不订阅的情况下直接使用内容（如果提供订阅）。
- SKU 名称未能准确体现订阅的性质，例如周期性自动收费的订阅含有“免费试用”或“试用 Premium 会员 - 免费 3 天”字样。
- 购买流程中的多个屏幕会导致用户误点击订阅按钮。
- 订阅产品未能提供持续性或周期性价值，例如在订阅期的第一个月提供 1000 个宝石，后续月份将福利减少为仅提供 1 个宝石。
- 要求用户必须注册自动续订才向其提供一次性福利，以及在用户购买后未收到用户的请求就取消其订阅。

示例 1：



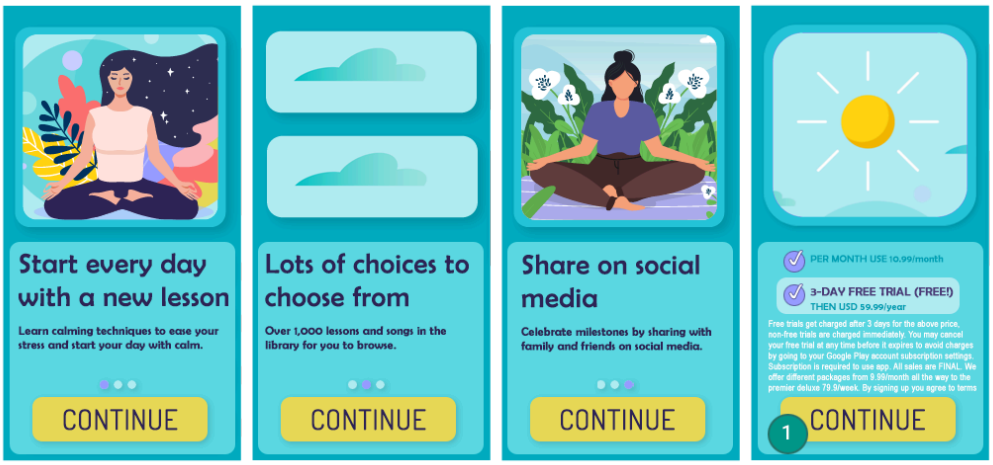
① 订阅方案页面没有清晰地显示“关闭”按钮，用户可能不知道可以在不订阅的情况下使用应用的功能。

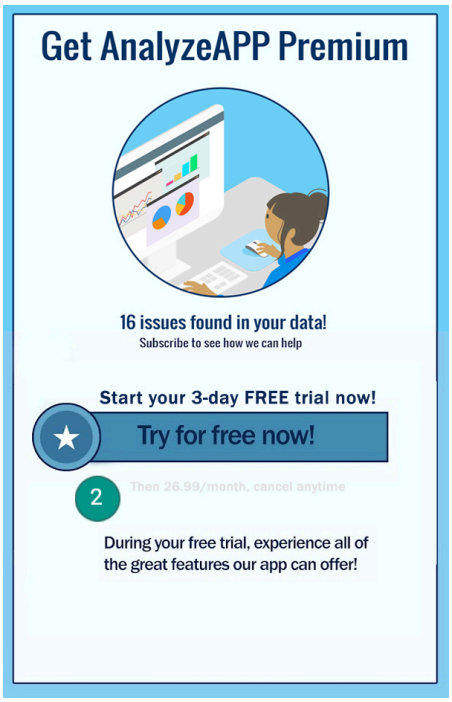
② 订阅方案仅显示以每月费用为单位的价格，用户可能不知道在订阅时系统会按六个月的价格收费。

③ 订阅方案仅显示初次体验价，用户可能不知道在初次体验期结束之后系统会自动按什么价格收费。

④ 订阅方案和条款及条件应本地化为同一种语言，以便用户理解整个订阅方案。

示例 2：





① 重复点击同一按钮区域导致用户意外点击最终的“继续”按钮，从而完成订阅。

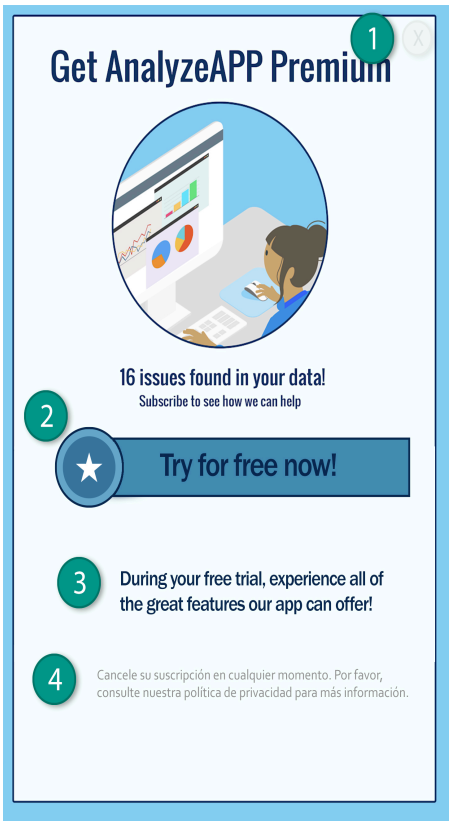
② 用户难以看清试用期结束后将会收取的金额，导致用户可能认为订阅方案是免费的。

免费试用和初次体验优惠

在用户订阅您的内容或服务之前：您必须清晰准确地说明订阅方案条款，包括用户可使用的内容或服务的期限、价格及说明。请务必告知用户免费试用的状态将在何时以何种方式转变为付费订阅、付费订阅的费用是多少，以及用户在试用结束后不想继续付费订阅时可以取消订阅。

下面是常见违规行为的一些示例：

- 优惠活动未明确说明用户可免费试用或享受初次体验价的期限。
- 优惠活动未明确说明系统会在优惠期结束时自动为用户开始付费订阅。
- 优惠活动未明确说明用户可以在不试用的情况下直接使用内容（如果提供试用）。
- 订阅方案的价格和条款未完全本地化。



①"关闭"按钮未清晰显示，用户可能不知道可以在不注册免费试用的情况下使用相关功能。

② 订阅方案着重强调免费试用，用户可能不知道试用结束后，系统会自动向他们收费。

③ 订阅方案未声明试用期，用户可能不知道他们能免费享受订阅内容多长时间。

④ 订阅方案和条款及条件应本地化为同一种语言，以便用户理解整个订阅方案。

订阅管理、取消和退款

如果您在应用中销售订阅内容，则必须确保应用明确披露用户可以如何管理或取消订阅。您还必须在应用中提供一种在线取消订阅的简易方法。在应用的帐号设置（或相应页面）中，您可以通过添加以下内容来满足此要求：

- 一个指向 Google Play 订阅中心的链接（适用于使用 Google Play 结算系统的应用）；和/或
- 直接进入取消流程的途径。

我们的一般政策规定，如果用户取消了通过 Google Play 的结算系统购买的订阅服务，那么无论在哪一天退订，都不会获得当前结算周期的退款，用户在当前结算期的剩余时间内会继续收到订阅内容。用户的取消订阅操作会从下一个结算周期开始生效。

作为内容或使用权限的提供者，您可以直接对用户实行更为灵活的退款政策。您有责任在您的订阅、订阅取消和退款政策发生变更时告知用户，同时也有责任确保这些政策符合适用法律的规定。

家庭自行认证广告 SDK 计划

如果您在应用内投放广告，且应用的目标受众群体只限于儿童（如家庭政策　所规定），那么您使用的广告 SDK 版本必须经过自行认证且符合 Google Play 政策，包括下文所述的家庭内容自行认证广告 SDK 计划相关要求。

如果应用的目标受众群体既包括儿童，也包括成人，则必须确保向儿童展示的所有广告均来自经自行认证的广告 SDK 版本（例如采用了无倾向年龄筛查措施）。

请注意，您有责任确保您在应用中实现的所有 SDK 版本均符合所有适用的政策以及当地法律法规，包括经自行认证的广告 SDK 版本。对于广告 SDK 在自行认证过程中提供的信息的准确性，Google 不提供任何声明或保证。

仅当您使用广告 SDK 面向儿童投放广告时，才需要使用经自行认证符合家庭政策要求的广告 SDK。如果广告 SDK 属于以下情况，则无需通过 Google Play 的自行认证即可获得准许；但您仍要负责确保您的广告内容和数据收集做法符合 Google Play 的用户数据政策 和家庭政策 。

- 用自家媒体资源投放自家广告 - 您使用 SDK 来管理各个应用间或应用与其他自有媒体和推销内容间的交叉推介。
- 已与广告主达成直接交易 - 使用 SDK 的目的是管理广告资源。

经自行认证符合家庭政策要求的广告 SDK

- 定义什么是令人反感的广告内容和行为，并在广告 SDK 的条款或政策中加以禁止。这些定义应符合 Google Play 开发者计划政策。
- 制定一套方法来根据相应的年龄段对广告素材进行分级。分级至少需要包含“所有人”和“成人”。分级方法必须与 Google 在 SDK 提供商填写以下申请表单后向其提供的方法一致。
- 允许发布商按个别请求或个别应用请求在面向儿童的内容中投放广告。此类广告投放必须遵守适用法律法规，例如美国的《儿童在线隐私保护法》(COPPA) 和欧盟的《一般数据保护条例》(GDPR) 。Google Play 要求广告 SDK 在面向儿童的内容中停用个性化广告、针对用户兴趣投放广告和再营销广告功能。
- 允许发布商选择符合 Google Play 的家庭政策中“广告和变现” 部分的广告格式，并满足教师认可计划 的要求。
- 确保在使用实时出价模式面向儿童投放广告时，广告素材经过审核，并且将隐私权声明传达给出价方。
- 向 Google 提供充足的信息以验证广告 SDK 的政策是否符合所有自行认证要求，例如提交测试应用以及通过下面的申请表单 提供信息；后续在 Google 要求您提供信息时及时回复，例如提供新版本以验证广告 SDK 版本符合所有自行认证要求。
- 进行自行认证 ，确保所有新版本均符合最新的 Google Play 开发者计划政策，包括家庭政策要求。

注意：经自行认证符合家庭政策要求的广告 SDK 在投放广告时，必须遵守所有可能适用于其发布商的儿童相关法律和法规。

如需详细了解如何为广告素材添加水印以及如何提供测试应用，请点击此处 。

以下是在通过广告投放平台向儿童投放广告时需遵守的要求：

- 仅使用经自行认证符合家庭政策要求的广告 SDK 或采取必要的保护措施，确保通过中介投放的所有广告均符合相关要求；并且
- 向中介平台传递必要的信息，指明广告内容分级和所有适用的面向儿童的内容。

开发者可以在此处 查看经自行认证符合家庭政策要求的广告 SDK 的列表，了解这些广告 SDK 的哪些具体版本经自行认证可以在家庭应用中使用。

此外，开发者还可以将此申请表单 分享给希望进行自行认证的广告 SDK。

商品详情和宣传

应用的宣传和曝光度会显著影响 Google Pay 商店的品质。因此，请避免使用包含垃圾内容的商品详情和品质低劣的宣传，也不得人为虚抬您的应用在 Google Play 中的曝光度。

应用宣传

我们不允许应用直接或间接参与对用户或开发者生态系统具有欺骗性或危害性的宣传活动（例如广告），也不允许应用从此类活动中直接或间接受益。如果宣传活动在行为或内容方面违反了我们的开发者计划政策，便具有欺骗性或危害性。

下面是常见违规行为的一些示例：

- 在网站、应用或其他资源中使用欺骗性　广告（包括使用类似于系统通知和提醒的通知）。
- 利用露骨色情　广告吸引用户前往应用的 Google Play 商品详情页面下载应用。
- 利用不当宣传或安装手法让用户在不知情的情况下被重定向至 Google Play 或开始应用下载进程。
- 通过短信服务强行进行宣传。
- 应用名称、图标或开发者名称中有文本或图片提及应用在商店内的表现或排名、价格或促销信息，或暗示与现有 Google Play 计划有关。

您有责任确保任何与您的应用相关联的广告网络、关联公司或广告均遵守这些政策。

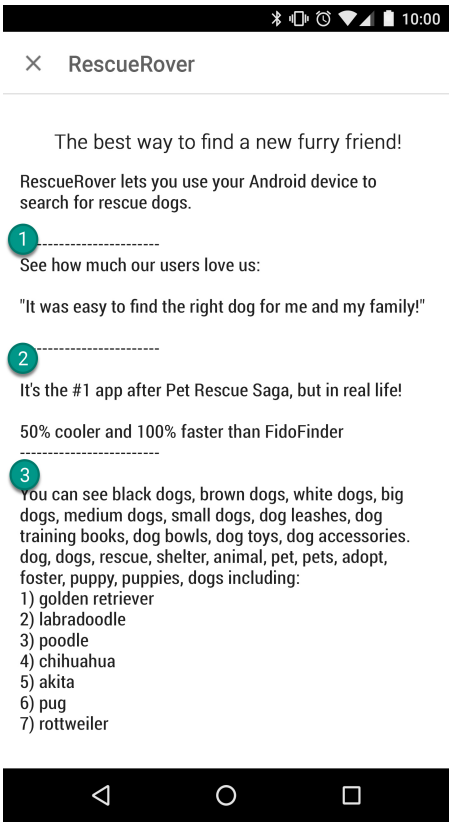
元数据

用户依赖应用说明来帮助了解应用的功能和用途。我们不允许任何应用中包含误导性、格式不正确、非描述性、不相关、过多或不恰当的元数据，包括但不限于应用的说明、开发者名称、名称、图标、屏幕截图和宣传图片。开发者必须提供针对其应用的精心构思的清晰说明。我们也不允许在应用的说明中展示未注明出处或匿名的用户赞誉。

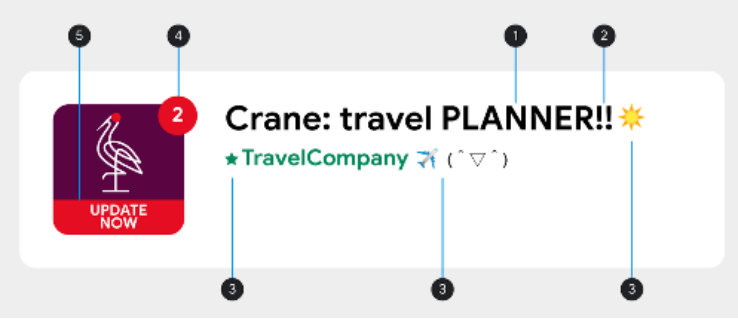
您的应用名称、图标和开发者名称非常有助于用户找到和了解您的应用。请勿在这些元数据元素中使用表情符号、表情符或重复使用特殊字符。除非是在品牌名称中，否则请避免使用全大写字母。应用图标中不得出现有误导性的符号，例如：在没有新消息的情况下显示代表有新消息的圆点标志，以及在与下载内容无关的应用中显示下载/安装符号。应用名称的长度不得超过 30 个字符。在应用名称、图标或开发者名称中使用的文本或图片不得涉及应用在商店内的表现或排名、价格或促销信息，也不得暗示与现有 Google Play 计划有关。

除了此处列出的要求之外，特定的 Google Play 开发者政策还可能要求您提供其他元数据信息。

下面是常见违规行为的一些示例：

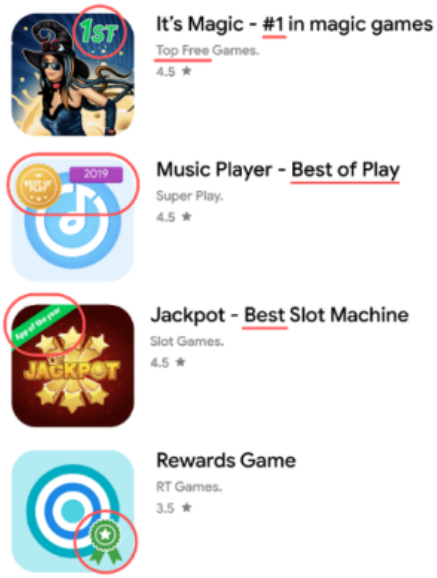


① 来源不明或匿名的用户赞誉
② 应用或品牌的数据对比信息
③ 字词堆砌及竖向/横向的字词罗列

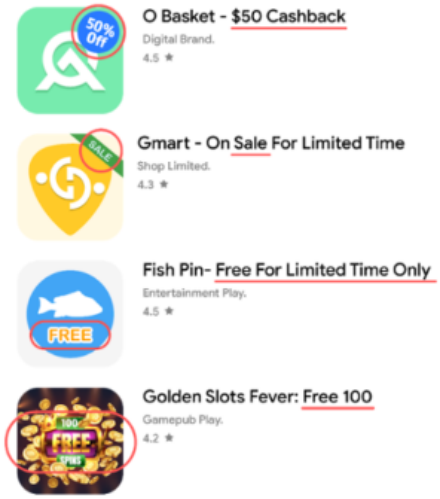


① 在品牌名称之外使用了全大写字母
② 与应用无关的一串特殊字符
③ 使用了表情符号、表情符（包括颜文字）和特殊字符
④ 有误导性的符号
⑤ 有误导性的文字

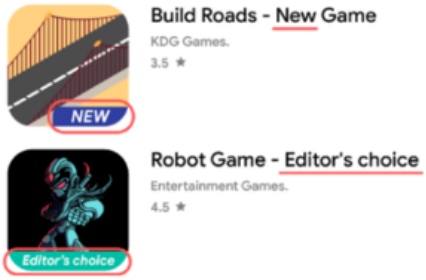
- 表明商店内表现/排名的图片或文本，例如“年度应用”“第一名”“20XX 年度 Play 应用”“热门”、奖项图标等。



- 表明价格和包含宣传信息的图片或文本，例如“九折优惠”“返现 50 元”“限时免费”等。



- 表明与各种 Google Play 计划有关的图片或文本，例如“编辑精选”“新上架”等。



下面是商品详情中存在不当文字、图片或视频的一些示例：

- 图像或视频包含挑逗性色情内容。请确保所使用的图像不具有挑逗性，不包含胸部、臀部、生殖器官或其他激起性欲的人体部位或内容（无论是绘制图还是实物图）。
- 在应用的商品详情中使用脏话、粗言秽语或其他不适合一般受众的语言。
- 应用图标、宣传图片或视频中含有醒目描绘的血腥暴力内容。
- 对非法用药的描绘。即便是商品详情中的教育、记录、科学或艺术 (EDSA) 内容，也必须适合所有受众群体。

下面列出了一些最佳实践：

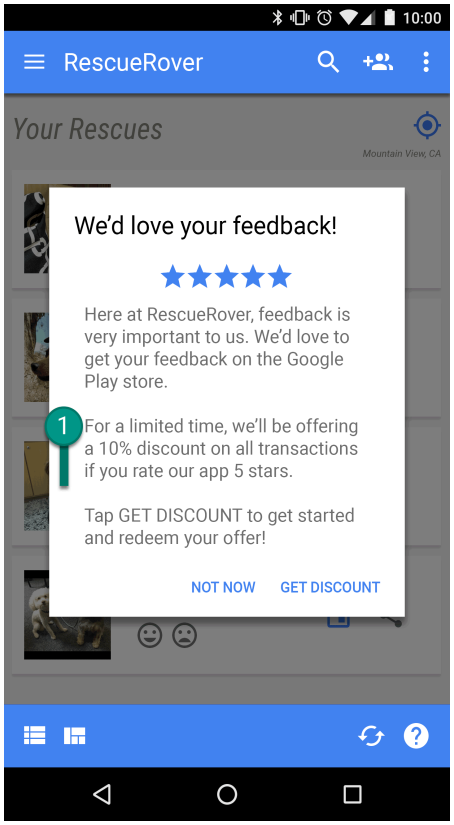
- 突出应用的亮点。介绍应用的有趣和精彩之处，从而帮助用户了解您的应用有何独到特色。
- 确保应用的名称和说明能够准确表述应用的功能。
- 避免使用重复或不相关的关键字或引用内容。
- 应用的说明务必要简洁明了。简短的说明往往可让用户的体验更佳，尤其在显示屏较小的设备上更是如此。应用说明过于冗长、太过详细、格式不正确或重复累赘都可能会违反此项政策。
- 请注意，商品详情应适合一般受众。请避免在商品详情中使用不当文字、图片或视频，并遵守上述指南。

用户评分、评价和安装次数

开发者不得试图操控任何应用在 Google Play 中的排名。这包括但不限于通过违规手段提升商品评分、评价或安装次数，例如通过欺诈或利诱手段获得评价和评分，或以利诱用户安装其他应用作为应用的主要功能。

下面是常见违规行为的一些示例：

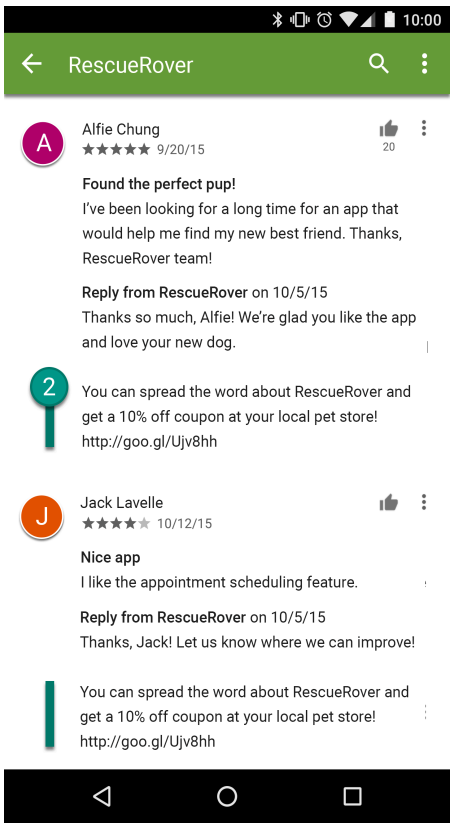
- 通过提供奖励要求用户为您的应用评分：



① 此通知向用户提供折扣优惠，借此换取较高的评分。

- 冒充用户重复提交评分，以影响应用在 Google Play 上的排名。

- 提交或鼓动用户提交包含不当内容的评价，此类内容包括联属营销信息、优惠券、游戏代码、电子邮件地址、网站链接或指向其他应用的链接：



② 此评价通过提供优惠券来鼓动用户宣传 RescueRover 应用。

评分和评价是衡量应用质量的基准，用户希望它们与应用紧密相关并且真实可靠。下面是回复用户评价的一些最佳实践：

- 回复时重点关注用户在评论中提出的问题；切勿要求用户给出更高的评分。
- 在回复中提供实用的资源，例如支持团队的联系地址或常见问题解答页面。

内容分级

Google Play 上的内容分级由国际年龄分级联盟 (IARC) 提供，旨在帮助开发者向用户显示符合当地情况的内容分级。区域性 IARC 部门制定了相关准则以用于确定应用内容对应的目标受众心智成熟度。我们不允许在 Google Play 上发布没有内容分级的应用。请注意，应用内出现的任何广告在内容受众心智成熟度方面一律不得显著高于应用自身的主要内容。如需了解详情，请参阅不恰当的广告 政策。

内容分级的用途

内容分级用于告知消费者（尤其是家长）应用中可能存在令人反感的内容。此外，内容分级还有助于系统依照相应法律要求在特定地区或面向特定用户过滤或屏蔽您的内容，以及确定您的应用是否符合加入特殊开发者计划的条件。

内容分级的指定方式

如需获得内容分级，您必须在 Play 管理中心填写分级调查问卷 ，其中的问题涉及应用内容的性质。系统会根据您在调查问卷中给出的回答，为您的应用指定多个分级机构提供的内容分级。对应用内容的虚假陈述可能会导致应用下架或遭到封停，因此请务必据实回答内容分级调查问卷中的问题。

为了避免系统将您的应用列为“未分级”，您必须为提交到 Play 管理中心的每个新应用以及目前已在 Google Play 上架的应用填写内容分级调查问卷。未进行内容分级的应用将会从 Play 商店下架。

如果您更改应用内容或功能，并且所做更改会影响您对分级调查问卷中问题的答案，您必须前往 Play 管理中心提交新的内容分级调查问卷。

向您的应用分配的内容分级专门针对应用内容，不考虑消费者协议或广告等其他功能和规范。您有责任向用户告知所有基于年龄的额外考虑因素，例如针对不同年龄群体的隐私权规范。

如需详细了解内容分级调查问卷，请前往帮助中心 了解各个区域的不同分级机构 以及如何完成内容分级调查问卷。

分级申诉

如果您对系统为应用指定的分级有异议，可以通过认证电子邮件中提供的链接直接向 IARC 分级机构提出申诉。

新闻与杂志

所有新闻与杂志应用都必须在 Google Play 管理中心内进行自我声明，并填写一份自我声明表单。

新闻与杂志应用是指符合以下条件的应用：

- 在 Google Play 管理中心内将自己声明为“新闻”或“杂志”类应用
- 或者列在 Google Play 商店的“新闻与杂志”类别中，并且在应用名称、图标、开发者名称或说明中将自身描述为“新闻”或“杂志”

如需进一步了解符合哪些条件的应用属于“新闻”或“杂志”类应用，请参阅针对新闻应用和新闻相关应用的要求。

此外，新闻与杂志应用必须符合以下条件：

- 提供新闻与杂志文章的来源，包括但不限于每篇文章的原始发布方或作者。

- 定期更新内容（无静态内容）。
- 让用户能够通过清晰便捷的方式获取应用的最新联系信息。
- 如果应用提供第三方内容（例如新闻与杂志聚合信息应用），必须向用户明确告知这些内容的发布来源。
- 让用户能在购买前预览应用内容（如果要求用户具有会员资格或订阅）。
- 不得以联属网络营销或赚取广告收入为主要目的。

垃圾内容、功能和用户体验

应用应为用户提供基本限度的适当功能和内容，带来引人入胜的用户体验。如果应用会崩溃、出现与预期用户体验不相符的其他行为，或者以向用户发送或在 Google Play 中提供垃圾内容为唯一目的，则不符合应用提供有效功能的标准。

垃圾内容

我们不允许任何应用向用户或 Google Play 提供垃圾内容，例如有以下行为的应用：向用户发送垃圾消息或邮件，或者提供重复或品质低劣的内容。

垃圾消息

我们不允许任何应用在未经用户确认内容和收件人的情况下，擅自以用户的名义发送短信、电子邮件或其他消息。

下面是常见违规行为的示例：

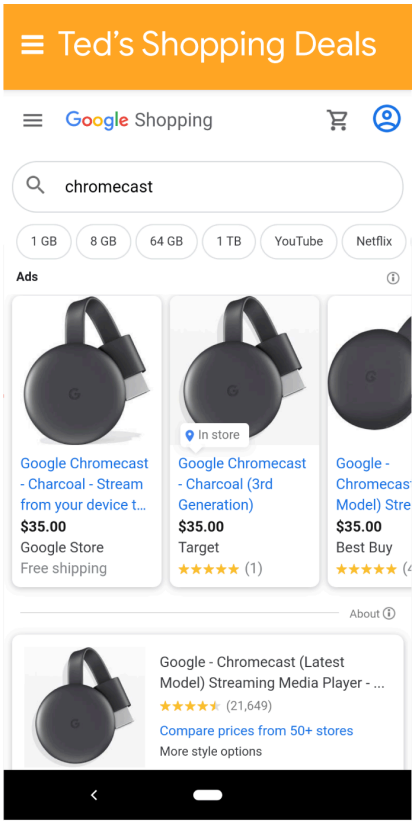
- 当用户按“分享”按钮时，应用在未经用户确认内容和接收人的情况下，擅自以用户的名义发送信息：

网页视图和联属营销企业垃圾内容

我们不允许主要用途为以下二者的应用：给某网站吸引引荐流量，或在未经网站所有者或管理员许可的情况下提供网站的网页视图。

下面是常见违规行为的一些示例：

- 主要用途是为某网站吸引引荐流量，从而凭借用户在该网站上注册或购买而获得收益的应用。
- 主要用途是在未经许可的情况下提供某网站的网页视图的应用：



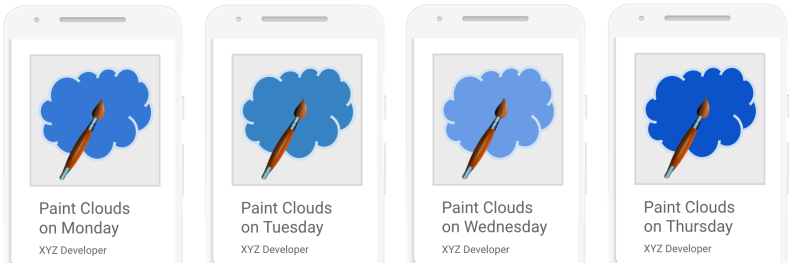
① 这款应用叫作“Ted's Shopping Deals”，它的功能就是单单提供 Google 购物的网页视图。

重复性内容

我们不允许任何应用纯粹提供与 Google Play 上已有的其他应用相同的体验。应用应提供独特的内容或服务，为用户带来价值。

下面是常见违规行为的一些示例：

- 复制其他应用的内容，且未添加任何原创内容或价值。
- 构建多款拥有高度相似的功能、内容和用户体验的应用。如果这些应用都只有少量内容，开发者应考虑构建一款整合了所有内容的应用。



功能、内容和用户体验

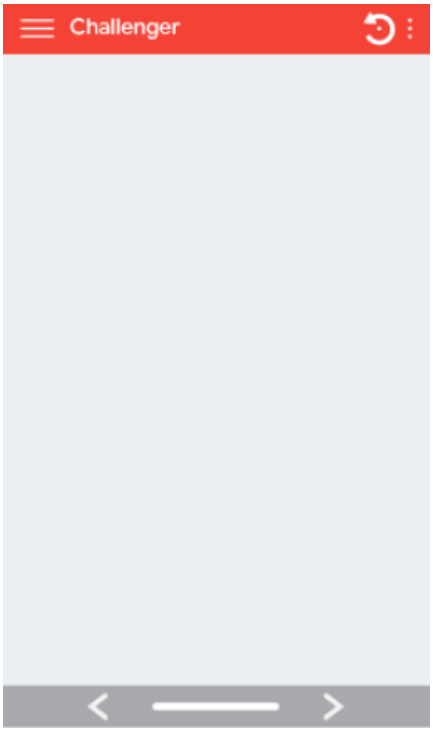
应用应当提供稳定、响应及时、引人入胜的用户体验。如果应用会崩溃、不具备移动应用应有的基本实用功能、缺乏引人入胜的内容，或出现与实用又引人入胜的用户体验不相符的其他行为，则不得在 Google Play 上架。

功能和内容有限

我们不允许仅提供有限功能和内容的应用。

下面是常见违规行为的示例：

- 没有专属功能的静态应用，例如仅支持文本或 PDF 文件的应用
- 内容非常少且未提供精彩用户体验的应用，例如单一壁纸应用
- 没有任何用途或功能的应用



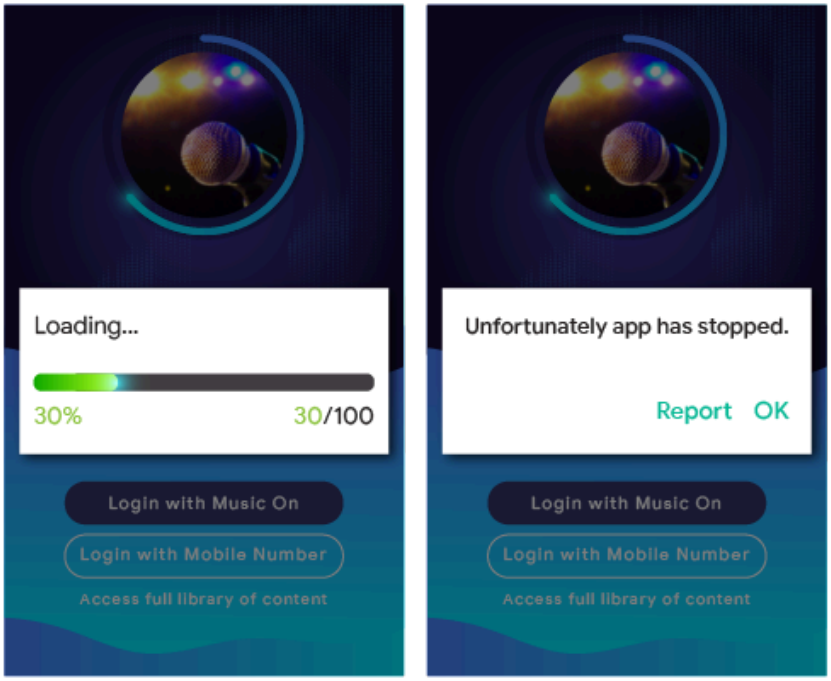
功能异常

我们不允许发布持续发生崩溃、强制关闭、卡住或其他功能异常情况的应用。

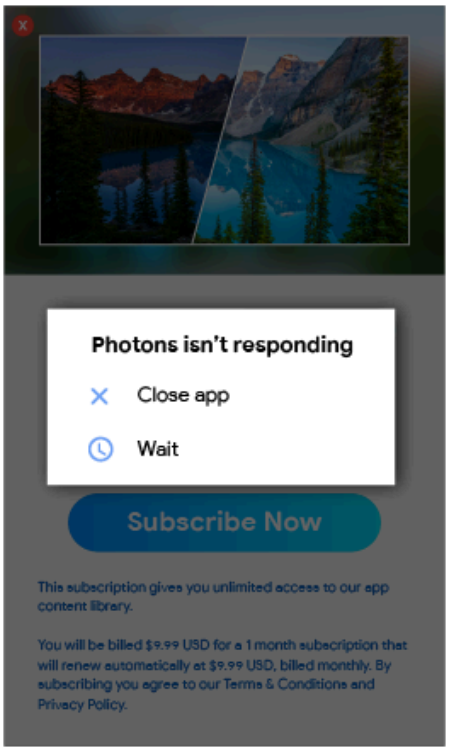
下面是常见违规行为的一些示例：

- 应用**无法安装**

- 应用可以安装，但**无法加载**



- 应用可以加载，但**无响应**



其他计划

开发者如果通过 Google Play 分发其他类别的 Android 应用，除需遵守本政策中心其他地方规定的内容政策外，还可能需要遵守特定计划的政策要求。请务必查看下方的列表，以确定您的应用是否适用其中任何政策。

Android 免安装应用

Android 免安装应用的开发宗旨是为用户打造愉悦、顺畅的用户体验，同时仍遵循最高的隐私权和安全标准。我们的政策就是为了实现这一宗旨而制定的。

如果开发者选择通过 Google Play 分发 Android 免安装应用，则必须遵守下列政策以及所有其他 Google Play 开发者计划政策。

身份信息

如果免安装应用包含登录功能，开发者必须集成 Smart Lock（密码专用）　。

链接支持

Android 免安装应用的开发者必须正确地支持指向其他应用的链接。如果开发者的免安装应用或安装式应用包含可能会打开其他免安装应用的链接，那么开发者必须将用户转到该免安装应用，而非采取其他处理方式（例如在 WebView　中显示相应链接）。

技术规范

开发者必须遵守 Google 制定的 Android 免安装应用技术规范和要求，包括我们的公开文档　中列出的规范和要求（Google 可能会不时进行修订）。

提供应用安装功能

免安装应用可向用户提供安装式应用，但不得以此为主要目的。开发者在提供安装功能时必须遵守以下规范：

- 在“安装”按钮上使用 Material Design“获取应用”图标　以及“安装”标签。
- 免安装应用中的隐含安装提示不得超过 2 到 3 次。
- 不得使用横幅或其他类似广告的技术向用户显示安装提示。

如需了解关于免安装应用的更多详细信息以及用户体验指南，请参阅用户体验最佳做法　。

更改设备状态

免安装应用不得对用户设备做出在免安装应用会话结束后仍将有效的更改。例如，免安装应用不得更改用户的壁纸，也不得创建主屏幕微件。

应用可见性

开发者必须确保免安装应用在运行期间始终对用户可见，以便用户知道免安装应用正在自己的设备上运行。

设备标识符

免安装应用不得存取同时满足以下两个条件的设备标识符：(1) 在免安装应用停止运行后仍然有效，且 (2) 不可由用户重置。相关示例包括但不限于：

- Build Serial
- 任何网络芯片的 MAC 地址
- IMEI、IMSI

免安装应用可以通过执行运行时权限获取电话号码。开发者不得试图利用这些标识符或以任何其他方式追踪用户。

网络流量

来自免安装应用内的网络流量必须使用传输层安全 (TLS) 协议（例如 HTTPS）进行加密。

Android 表情符号政策

我们的表情符号政策旨在促进提供包容且一致的用户体验。为了达成这个目标，凡是在 Android 12 或更高版本上运行的应用，都必须支持最新版 Unicode 表情符号 。

如果应用在 Android 12 或更高版本上运行，而且使用默认 Android 表情符号，没有任何自定义实现，便已使用最新版 Unicode 表情符号。

如果应用在 Android 12 或更高版本上运行，且实现了自定义表情符号（包括由第三方库提供的表情符号），当新的 Unicode 表情符号推出后，应用必须在 4 个月内完全支持最新的 Unicode 版本。

请参阅这份指南 ，了解如何支持新式表情符号。

家庭

Google Play 为开发者提供了一个丰富实用的平台，让开发者能够展示适合全家人的优质内容。在向亲子同乐计划提交应用或向 Google Play 商店提交面向儿童的应用之前，您应先确保自己的应用适合儿童且符合所有相关法律的规定。

前往应用开发学习学院了解与家庭政策和要求相关的流程并查看互动式核对清单。

Google Play 家庭政策

如今，越来越多的家庭开始利用科技来丰富家庭生活，家长们在寻找安全优质的内容来与孩子们分享。您的应用也许是专为儿童设计，也可能只会引起他们的注意。Google Play 希望协助您确保应用对所有用户而言都是安全的，包括家庭用户。

“儿童”一词在不同的语言区域和语境中具有不同的含义。请务必咨询您的法律顾问，确定您的应用可能需要遵守的义务和/或年龄限制。您对自己应用的用途了解得最清楚，因此需要您协助我们确保 Google Play 上的应用适合全家共享。

对于所有符合 Google Play 家庭政策的应用，其开发者都可以选择申请教师认可计划的评级，但我们不能保证您的应用一定可以加入教师认可计划。

Play 管理中心要求

目标受众群体和内容

发布应用之前，您必须在 Google Play 管理中心的目标受众群体和内容 部分提供的年龄段列表中选择应用的目标受众群体。无论您在 Google Play 管理中心内选择哪个选项，只要您的应用包含可被视为面向儿童的图像和术语，就可能会影响 Google Play 对您声明的目标受众群体所给予的评估结果。Google Play 保留自行审核您提供的应用信息，以判断您披露的目标受众群体是否准确的权利。

如果选择将多个年龄段作为应用的目标受众群体，您必须确保应用是专为所选年龄段的用户设计的，且确实适合这些用户。例如，如果是专为婴幼儿和学龄前儿童设计的应用，则只应将“5 岁及以下”年龄段作为此类应用的目标受众群体。如果您的应用是专为特定年级的学生用户而设计，请选择最能代表相应年级的年龄段。如果您的应用确实专为所有年龄段的用户而设计，则只应选择同时包含成人和儿童的年龄段。

更新“目标受众群体和内容”部分

您随时可以在 Google Play 管理中心的“目标受众群体和内容”部分更新应用的信息。您必须提交应用更新 ，相应信息才会体现在 Google Play 商店中。不过，Google 可能会在您提交应用更新之前，就先行审核您在 Google Play 管理中心的这个部分变更的任何内容，确认是否符合政策规定。

如果您更改了应用的目标受众群体年龄段，或开始使用广告或应用内购买功能，我们强烈建议您通过应用详情页面的“新功能”部分或应用内通知，向现有用户告知这些变动。

在 Play 管理中心提供虚假陈述

如果您在 Play 管理中心为应用提供的信息（包括“目标受众群体和内容”部分的信息）有任何虚假陈述，可能会导致应用遭到下架或封停，因此请务必据实提供信息。

家庭政策要求

如果应用的目标受众群体包括儿童，则必须遵守下列要求，否则可能会导致应用遭到下架或暂停。

1. **应用内容：**您的应用中可供儿童访问的内容必须适合儿童。如果应用中有的内容在全球某些地区属于不当内容，但在特定地区被认定为适合儿童用户，那么该应用或许可在该地区上架（地区限制），但在其他地区仍无法上架。
2. **应用功能：**未经某个网站的所有者或管理员许可，您的应用不能以提供该网站的 WebView 为唯一目的，也不能以为该网站吸引联属营销流量为主要目的。
3. **在 Play 管理中心回答问题：**您必须在 Play 管理中心内据实回答有关应用的问题；如果应用有所变化，还应更新回答内容，如实反映相应变化。这包括但不限于在“目标受众群体和内容”部分、“数据安全”部分和 IARC 内容分级调查问卷中针对您的应用提供准确的回答。
4. **数据方面的做法：**如果您的应用会向儿童收集任何个人信息和敏感信息（包括通过应用调用或使用的 API 和 SDK 收集），您必须在应用中披露这一行为。儿童敏感信息包括但不限于身份验证信息、麦克风和相机传感器数据、设备数据、Android ID 以及广告使用情况数据。您还必须确保应用遵循以下数据方面的做法：
   - 专门面向儿童的应用不得传输 Android 广告标识符 (AAID)、SIM 卡序列号、版本序列号、BSSID、MAC、SSID、IMEI 和/或 IMSI。
     - 专门面向儿童的应用在以 Android API 33 或更高版本为目标平台时不得请求 AD_ID 权限。
   - 如果应用的目标对象同时包括儿童和年龄更大的用户，则应用不得传输从儿童或不确定年龄的用户处获取的 AAID、SIM 卡序列号、版本序列号、BSSID、MAC、SSID、IMEI 和/或 IMSI。
   - 不得通过 Android API 的 TelephonyManager 索取设备电话号码。
   - 专门面向儿童的应用不得请求位置信息权限，也不得收集、使用或传输确切位置信息。
   - 除非您的应用仅支持不兼容配套设备管理器 (CDM)　的设备操作系统版本，否则应用申请蓝牙权限时，必须使用 CDM。
5. **API 和 SDK：**您必须确保应用以适当的方式使用所有 API 和 SDK。
   - 专门面向儿童的应用不得包含未获准用于主要面向儿童的服务的任何 API 或 SDK，
     - 例如，某 API 服务使用 OAuth 技术进行身份验证和授权，而其服务条款声明其未获准用于面向儿童的服务。
   - 如果应用的目标对象同时包括儿童和年龄更大的用户，则应用不得使用未获准用于面向儿童的服务的 API 或 SDK，除非这样的 API 或 SDK 是与无倾向年龄筛查搭配使用，或采用不会收集儿童数据的方式实现。如果应用的目标对象同时包括儿童和年龄更大的用户，则应用不得要求用户通过未获准用于面向儿童的服务的 API 或 SDK 访问应用内容。
6. **增强现实 (AR)：**如果应用采用增强现实技术，那么您必须确保在启动 AR 部分时会立即显示安全警告。警告应包含以下信息：
   - 适当提醒家长需要对孩子使用应用的情况加以监督。
   - 提醒用户留意现实环境中的危险因素（例如注意周围的环境）。
   - 您的应用不得要求使用不建议儿童操作的设备（例如 Daydream 和 Oculus）。
7. **社交应用和功能：**如果您的应用可让用户分享或交换信息，您必须在 Play 管理中心的内容分级调查问卷中准确披露这些功能。
   - 社交应用：社交应用是指主要用途是让用户能够与大规模群体分享任意格式的内容或与之交流的应用。只要社交应用的目标受众群体包括儿童，就必须在允许儿童用户交换任意格式的媒体内容或信息之前，通过应用内消息提醒他们注意上网安全并了解线上互动带来的实际风险。您还必须要求成人执行某项操作，然后才能允许儿童用户交换个人信息。
   - 社交功能：社交功能是指让用户能够与大规模群体分享任意格式的内容或与之交流的任何附加应用功能。只要应用的目标受众群体包括儿童并且提供社交功能，就必须在允许儿童用户交换任意格式的媒体内容或信息之前，通过应用内消息提醒他们注意上网安全并了解线上互动带来的实际风险。您还必须提供一种方法供成人管理面向儿童用户的社交功能，包括但不限于启用/停用社交功能或选择不同级别的功能。最后，您还必须要求成人执行相关操作，然后才能启用允许儿童交换个人信息的功能。
   - 成人操作是一种机制，用于验证用户并非儿童，并且可以避免儿童通过虚报年龄的方式获得访问应用成人专区的权限。具体的措施包括，要求提供成人 PIN 码、密码、出生日期、带照片的身份证件、信

用卡、社会保障号 (SSN)，或进行电子邮件验证。
  - 如果社交应用的主要用途是与陌生人聊天，则不得以儿童为目标对象。示例包括：聊天轮盘类应用、约会应用、主要面向儿童的开放聊天室等。
8. **符合法律规定：**您必须确保应用（包括应用调用或使用的 API 或 SDK）符合美国《儿童在线隐私保护法》(COPPA) 、欧盟《一般数据保护条例》(GDPR) ，以及任何其他适用法律或法规的规定。

下面是常见违规行为的一些示例：

- 应用的商品详情中宣称适合儿童玩，但应用内容只适合成人。
- 应用使用了特定 API，但该 API 在服务条款中规定不得将其用于面向儿童的应用。
- 应用美化饮用酒精饮料、吸食烟草制品或使用管制药品的行为。
- 应用包含实际或模拟赌博的内容。
- 应用中包含不适合儿童的暴力、血腥或惊悚内容。
- 应用中提供交友服务、性爱建议或婚姻建议。
- 应用包含指向某些网站的链接，这些网站提供的内容违反了 Google Play 的开发者计划政策 。
- 应用向儿童展示成人广告（例如暴力内容、色情内容、赌博内容）。

广告和获利

如果您要通过 Google Play 上某款面向儿童的应用创收，则该应用必须遵守家庭政策中“广告和创收”部分的以下要求。

以下政策适用于您的应用中的所有创收和广告内容，包括广告、交叉推介内容（对于您的应用和第三方应用）、应用内购优惠或任何其他商业内容（例如付费产品植入）。此外，这类应用中的所有创收和广告内容都需遵守所有适用的法律法规（包括任何相关的自律准则或行业准则）。

Google Play 有权拒绝、下架或暂停采取激进商业策略的应用。

广告要求

如果您的应用会面向儿童或不确定年龄的用户展示广告，您必须：

- 仅使用已加入 Google Play 家庭内容自行认证广告 SDK 计划的广告 SDK 向这些用户展示广告；
- 确保向这些用户展示的广告不涉及针对用户兴趣投放广告的行为（根据用户的在线浏览行为面向具有某些特征的个人用户投放广告）或再营销行为（根据用户之前与某个应用或网站的互动情况面向个人用户投放广告）；
- 确保向这些用户展示的广告所呈现的内容适合儿童；
- 确保向这些用户展示的广告符合家庭广告格式要求；并且
- 确保遵守与面向儿童投放广告相关的所有适用法规和行业标准。

广告格式要求

应用中的变现和广告内容不得包含欺骗性内容，也不得采用会导致儿童用户无意中点击的设计。

如果应用的目标受众群体只限于儿童，则不得出现以下行为：如果应用的目标受众群体覆盖儿童和成人，那么在向儿童或不确定年龄的用户投放广告时不得出现以下行为：

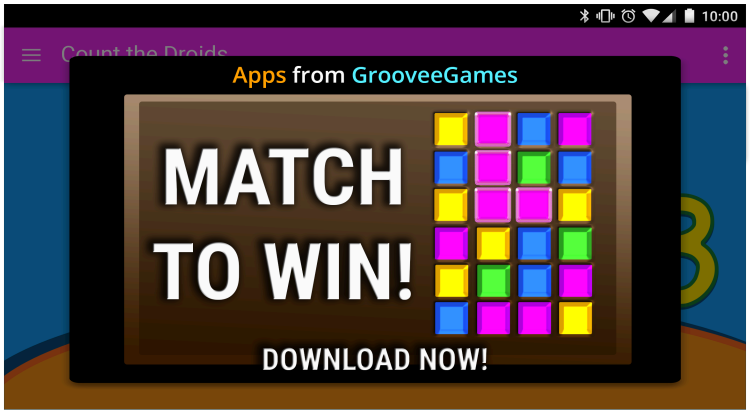
- 投放干扰性变现和广告内容，包括会占据整个屏幕或干扰正常使用，且未明确提供广告关闭方式的变现和广告内容（例如广告墙）。
- 干扰用户正常使用应用或玩游戏的变现和广告内容（包括 5 秒过后仍无法关闭的激励广告或主动观看广告）。
- 变现和广告内容不会干扰用户正常使用应用或玩游戏，但会持续展示 5 秒以上（例如，包含集成广告的视频内容）。
- 在应用启动后随即展示插页式变现和广告内容。
- 一个网页上出现多个广告展示位置。例如，横幅广告在一个展示位置展示多项优惠，或同时展示多个横幅广告或视频广告，这些都是不允许的。
- 投放难以与应用内容区分的变现和广告内容，例如积分墙或其他沉浸式广告体验。

- 利用令人震惊或情感操纵的伎俩促使用户查看广告或进行应用内购买。
- 投放通过以下方式强制用户点击的欺骗性广告：使用关闭按钮触发其他广告，或让广告突然出现在应用中通常供用户点按访问其他功能的区域。
- 未区分使用虚拟游戏币和现金购买应用内购商品的行为。

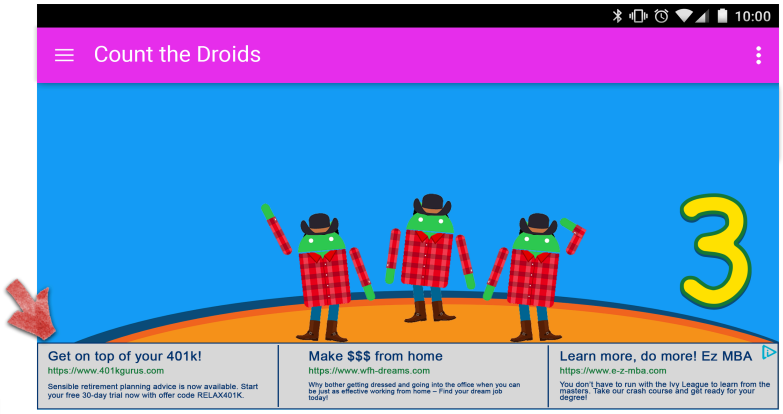
下面是常见违规行为的一些示例：

- 创收和广告内容在用户尝试将其关闭时移到其他位置
- 创收和广告内容在五 (5) 秒后仍未提供让用户关闭优惠信息的方式，如下方的示例所示：

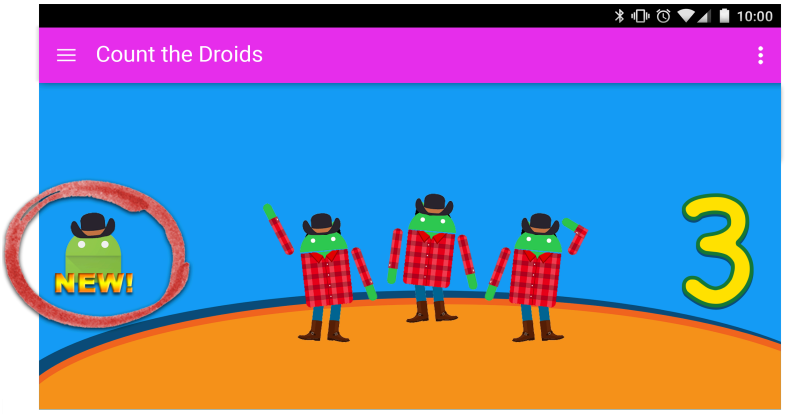
- 创收和广告内容占据大部分或整个设备屏幕，且未为用户提供明确的关闭方法，如下所示：



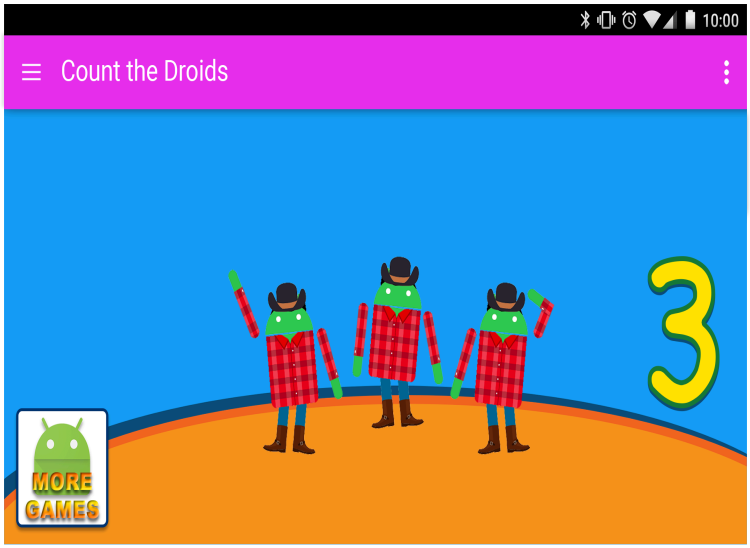
- 横幅广告中显示多条小广告，如下所示：



- 创收和广告内容可能会让用户误认为是应用内容，如下所示：



- 按钮、广告或其他创收内容宣传您的其他 Google Play 商品详情信息，但难以与应用内容区分，如下所示：



以下是一些不应向儿童展示的不当广告内容示例。

- **不当媒体内容**：在广告中宣传儿童不宜的电视节目、电影、音乐专辑或任何其他媒体内容。
- **不当视频游戏和可下载软件**：在广告中宣传儿童不宜的可下载软件及电子视频游戏。
- **管制类物品或有害物品**：在广告中宣传酒精饮料、烟草制品、管制类物品或任何其他有害物品。
- **赌博**：在广告中宣传模拟赌博、竞赛或抽奖促销（即使可免费参与也不允许）。
- **成人内容和性暗示内容**：广告内含色情、性暗示和少儿不宜的内容。
- **约会或交友**：在广告中宣传约会或成人交友网站。

- **暴力内容**：广告内含儿童不宜的血腥暴力内容和画面。

广告 SDK

如果您在应用内投放广告，且应用的目标受众群体只限于儿童，那么您必须仅使用已加入家庭内容自行认证广告 SDK 计划的版本。如果应用的目标受众群体既包括儿童，也包括成人，则必须采取年龄筛查措施（例如无倾向年龄筛查），并确保向儿童展示的所有广告均来自已加入 Google Play 自行认证广告 SDK 计划的版本。

请参阅"家庭内容自行认证广告 SDK 计划"政策页面，详细了解相关要求；您还可以前往此处查看目前已加入家庭内容自行认证广告 SDK 计划的版本列表。

如果您使用 AdMob，请参阅 AdMob 帮助中心，详细了解相关产品。

您有责任确保应用符合与广告、应用内购和商业内容相关的所有要求。如需详细了解您的广告 SDK 提供商的内容政策和广告做法，请与相应提供商联系。

家庭内容自行认证广告 SDK 政策

Google Play 致力于为儿童和家庭打造安全可靠的用户体验。其中关键的一点是确保儿童只会看到适合其年龄段的广告，并且他们的数据会得到妥善处理。为实现这一目标，我们要求广告 SDK 和中介平台自行证明其适合儿童，且符合 Google Play 开发者计划政策 和 Google Play 家庭政策，包括家庭内容自行认证广告 SDK 计划的相关要求。

Google Play 家庭内容自行认证广告 SDK 计划是一种重要的验证方式，开发者可以通过该计划判断哪些广告 SDK 或中介平台已自行证明其适合在专为儿童设计的应用中使用。

如果您提供的 SDK 相关信息有任何虚假陈述，您的 SDK 可能会因此被移出家庭内容自行认证广告 SDK 计划或遭暂停，因此请务必据实提供信息，包括您在申请表单中提供的信息。

政策要求

如果您的 SDK 或中介平台所服务的应用加入了 Google Play 亲子同乐计划，您必须遵守所有 Google Play 开发者政策，包括以下要求。违反任何政策要求都可能会导致 SDK 或中介平台被家庭内容自行认证广告 SDK 计划除名，或被暂停参与该计划。

您有责任确保您的 SDK 或中介平台符合相关规定，因此请务必查看Google Play 开发者计划政策、Google Play 家庭政策和家庭内容自行认证广告 SDK 计划要求。

1. **广告内容：**如果您的广告内容可供儿童访问，则必须适合儿童。
   - 您必须 (i) 定义什么是令人反感的广告内容和行为，并 (ii) 在相关条款或政策中禁止此类内容和行为。相关定义应符合 Google Play 开发者计划政策的规定。
   - 您还必须制定一种方法来根据相应的年龄段对广告素材进行分级。分级至少需要包含"适合所有人"和"适合成人"。分级方法必须与 Google 在 SDK 提供方填写意向调查表后向其提供的方法一致。
   - 您必须确保在使用实时出价模式向儿童投放广告时，广告素材已经过审核且符合上述要求。
   - 此外，您必须采用特定机制来直观标识来自您的广告资源的广告素材，例如为相应广告素材添加贵公司的视觉徽标水印，或采用类似功能。
2. **广告格式：**您必须确保向儿童用户展示的所有广告都符合家庭内容广告格式要求，并且您必须允许开发者选择符合 Google Play 家庭政策的广告格式。
   - 广告不得包含欺骗性内容，也不得采用会导致儿童用户无意中点击的设计。不得投放通过以下方式强制用户点击的欺骗性广告：利用关闭按钮触发其他广告；或让广告突然出现在应用中通常供用户点按访问其他功能的区域。
   - 不得投放干扰性广告，包括会占据整个屏幕画面或干扰用户正常使用应用、且未明确提供关闭方式的广告，例如广告墙。
   - 干扰用户正常使用应用或玩游戏的广告（包括激励广告或用户选择观看的广告）在 5 秒后必须可以关闭。

- 一个页面上不得出现多个广告展示位置。例如，不得投放在一个展示位置显示多项优惠的横幅广告，也不得同时展示多个横幅广告或视频广告。
- 广告与应用内容之间必须有明显的区别。不得投放儿童用户不能明确辨认为广告的积分墙或沉浸式广告体验。
- 广告不得利用令人震惊或操纵情感的伎俩诱导用户查看其内容。

3. **IBA/再营销：**您必须确保向儿童用户展示的广告不涉及针对用户兴趣投放广告，也不涉及再营销。针对用户兴趣投放广告是指根据具有某些特征的个别用户的在线浏览行为，向这些用户投放广告；再营销是指根据个别用户之前与某个应用或网站的互动情况，向这些用户投放广告。
4. **数据方面的做法：**作为 SDK 提供方，您必须清楚说明您会如何处理用户数据（例如从用户那里收集的信息或收集的与用户有关的信息，包括设备信息）。也就是说，您必须披露您的 SDK 访问、收集、使用及分享数据的方式，而且数据使用范围必须仅限于已披露的用途。除了这些 Google Play 要求之外，您还需遵守适用的隐私保护和数据保护法律规定的要求。如果您的 SDK 会从儿童那里收集任何个人信息和敏感信息，包括但不限于身份验证信息、麦克风和摄像头传感器数据、设备数据、Android ID 以及广告使用情况数据，您必须披露这一行为。
   - 您必须允许开发者根据每个请求或每个应用的具体情况，就广告投放提出按面向儿童的内容进行处理的请求。此类处理必须遵守适用法律法规，例如美国《儿童在线隐私保护法》(COPPA) 和欧盟《一般数据保护条例》(GDPR) 。
     - Google Play 规定，广告 SDK 不得在面向儿童的内容中投放个性化广告、针对用户兴趣投放广告以及进行再营销。
   - 您必须确保在使用实时出价模式向儿童投放广告时，将隐私指示标志传达给出价方。
   - 不得传输从儿童或年龄未知的用户那里获取的 AAID、SIM 卡序列号、版本序列号、BSSID、MAC、SSID、IMEI 和/或 IMSI。
5. **中介平台：**向儿童投放广告时，必须遵循以下要求：
   - 仅使用家庭内容自行认证广告 SDK 或采取必要的保护措施，确保通过中介投放的所有广告均符合相关要求；并且
   - 向中介平台传递必要的信息，指明广告内容分级和所有适用的面向儿童的内容。
6. **自行认证和合规性**：您必须向 Google 提供足够的信息，例如此意向调查表 中指出的信息，以便 Google 验证广告 SDK 是否符合所有自行认证要求，包括但不限于：
   - 提供 SDK 或中介平台的英文版服务条款、隐私权政策和发布商集成指南
   - 提交示例测试应用。该应用必须使用最新的合规版广告 SDK，应该是完整构建的可执行 Android APK，并且使用相应 SDK 的所有功能。测试应用需满足的要求：
     - 提交的测试应用必须是完整构建的可执行 Android APK，并且能够在手机上运行。
     - 使用的广告 SDK 必须是最新发布的版本或即将发布的版本，并且符合 Google Play 政策。
     - 必须使用您的广告 SDK 的所有功能，包括调用广告 SDK 来获取和展示广告。
     - 必须能够通过在测试应用中请求获得的广告素材，覆盖广告网络中当前所有可用/可投放的广告资源。
     - 不得受地理位置的限制。
     - 如果您的广告资源面向多个年龄段的受众群体，那么测试应用必须能够区分哪些广告素材请求来自整体广告资源，哪些广告素材请求来自适合儿童或适合所有年龄段用户的广告资源。
     - 除非应用受到无倾向年龄筛查机制的约束，否则不得仅限于在相应广告资源中投放特定广告。
7. 您必须在收到任何索取信息的后续请求时及时回复，并进行自行认证 ，确保所有新发布的版本均符合最新的 Google Play 开发者计划政策，包括家庭政策要求。
8. **符合法律规定：**如果广告投放符合所有涉及儿童、可能适用于相应发布商的相关法令和法规，家庭内容自行认证广告 SDK 必须支持此类广告投放。
   - 您必须确保您的 SDK 或中介平台符合美国《儿童在线隐私保护法》(COPPA) 、欧盟《一般数据保护条例》(GDPR) 以及所有其他适用法律法规。

     注意：“儿童”一词在不同的语言区域和语境中可能具有不同的含义。请务必咨询您的法律顾问，以便确定您的应用可能需要履行的义务和/或遵守的年龄相关限制。您最清楚自己的应用的运作机制，因此我们需要您协助确保 Google Play 上的应用适合全家共享。

请参阅家庭内容自行认证广告 SDK 计划页面，详细了解该计划的要求。

执行

避免政策违规行为总比事后补救要好，但当应用确实存在违规行为时，我们会尽全力确保开发者了解如何修正其应用以符合相关规定。如果您发现任何违规行为 ，或者对管理违规行为 有任何疑问，请告知我们。

政策覆盖范围

我们的政策适用于您的应用所显示或链接到的任何内容，包括您的应用向用户显示的任何广告，以及您的应用所托管或链接到的任何用户制作的内容。此外，这些政策还适用于 Google Play 上您的开发者帐号名下公开显示的任何内容，包括您的开发者名称，以及您所列出的开发者网站的着陆页。

我们不允许任何应用让用户在其设备上安装其他应用。如果某个应用让用户无需安装即可访问其他应用、游戏或软件（包括第三方提供的功能和体验），则开发者必须确保该应用提供访问权限的所有内容均符合各项 Google Play 政策，而且这些内容可能还需要接受其他的政策审核。

这些政策中所用术语的含义与开发者分发协议 (DDA) 中所用术语的含义相同。除了遵守这些政策和《开发者分发协议》外，您还必须根据我们的内容分级指南对您的应用内容进行分级。

我们不允许任何应用或应用内容破坏用户对 Google Play 生态系统的信任。在评估是否在 Google Play 中上架或下架应用时，我们会考虑多种因素，包括但不限于有害行为模式或高滥用风险。我们会根据许多因素识别滥用风险，考虑的因素包括但不限于针对具体应用和开发者的投诉、新闻报道、以前的违规记录、用户反馈以及使用热门品牌、角色和其他资产的行为。

Google Play 保护机制的运作方式

Google Play 保护机制会在您安装应用时对应用进行检查，还会定期扫描您的设备。如果此保护机制发现潜在有害应用，可能会执行以下操作：

- 向您发送通知。如需移除相应应用，请点按该通知，然后点按卸载。
- 停用该应用，直到您将其卸载。
- 自动移除该应用。在大多数情况下，如果检测到有害应用，您会收到一则通知，告知您该应用已被移除。

恶意软件防护功能的运作方式

为保护您免遭受第三方恶意软件、有害网址和其他安全问题的侵害，Google 可能会接收与以下内容相关的信息：

- 您设备的网络连接
- 可能有害的网址
- 操作系统以及通过 Google Play 或其他来源安装在您设备上的应用。

Google 可能会就不安全的应用或网址向您发出警告。如果 Google 确认某个应用或网址会对设备、数据或用户造成危害，则可能会移除该应用或阻止您安装该应用，以及阻止您访问此网址。

您可以在设备设置中选择停用部分防护功能。不过，Google 可能会继续接收关于通过 Google Play 安装的应用的信息，并且可能会继续检查通过其他来源安装在您设备上的应用，以确定是否存在安全问题（但不会将相关信息发送给 Google）。

隐私提醒的运作方式

如果某个应用已从 Google Play 商店下架，这意味着该应用可能存在访问您个人信息的行为，Google Play 保护机制会提醒您，而您可以选择将其卸载。

执行流程

在审核内容或账号是否违法或违反我们的政策时，我们会在做最终判定前考虑各种信息，包括应用元数据（例如应用名称、说明）、应用内体验、账号信息（例如过往的违规记录）、应用内的任何第三方代码、通过报告机制（如果适用）提供的其他信息，以及自发审核信息。请注意，您有责任确保您的应用内使用的第三方代码（例如某个 SDK）以及该第三方针对您的应用采取的做法均符合所有 Google Play 开发者计划政策。

如果您的应用或开发者帐号违反任一政策，我们会根据具体情况采取下列处置措施。此外，我们还会通过电子邮件向您提供我们所采取处置措施的相关信息，以及申诉说明（如果您认为我们的处置措施有误，可以按照说明申诉）。

请注意，下架通知或管理通知中可能不会一一指出您的帐号、应用或所属应用目录中出现的每项违反政策的行为。开发者有责任处理所有政策问题，并进一步核查，以确保应用或帐号的其余部分完全符合政策规定。如果您未能解决您的帐号和所有应用中违反政策的行为，我们可能会采取其他违规处置措施。

如果您屡次或严重违反（例如应用含有恶意软件、存在欺诈行为以及可能危害到用户或设备）这些政策或开发者分发协议 (DDA)，您的开发者帐号或相关的 Google Play 开发者帐号可能会被终止。

违规处置措施

不同的违规处置措施会对您的应用产生不同的影响。我们结合使用人工与自动化评估机制来审核应用及应用内容，检测和评估哪些内容违反政策并会对用户和整个 Google Play 生态系统造成伤害。使用自动化模型有助于我们检测更多违规行为和更快地评估潜在问题，从而确保 Google Play 为所有人打造安全的使用体验。自动化模型会移除违反政策的内容，但如果需要更缜密的审查（例如需要了解内容的上下文）才能判定，模型会为内容添加标记，交由负责内容评估并且经过培训的操作人员和分析人员评估。然后，我们会利用人工审核的结果来构建训练数据，以进一步改进机器学习模型。

以下部分介绍了 Google Play 可能采取的各种处置措施，以及这些措施会对您的应用和/或您的 Google Play 开发者帐号产生的影响。

除非违规处置通知中另有说明，否则这些处置措施会影响所有地区。例如，如果您的应用被暂停，该应用在所有地区均无法提供。此外，除非另有说明，否则这些处置措施将持续有效，直到您对处置措施提出申诉并获得批准为止。

被拒

- 提交审核的新应用或应用更新不会在 Google Play 上发布。
- 如果对现有应用的更新被拒，则更新之前发布的应用版本仍会保留在 Google Play 上。
- 被拒不会影响您访问被拒绝应用的现有用户安装量、统计信息和评分。
- 被拒不会影响您的 Google Play 开发者帐号的信誉。

注意：在解决所有违反政策的行为之前，请勿尝试重新提交被拒的应用。

下架

- 该应用（包括之前的所有版本）都会从 Google Play 中下架，用户将无法再下载该应用。
- 应用下架后，用户将无法查看应用的商品详情。只要您针对已下架的应用提交了符合政策的更新，这些信息就会恢复。
- 在 Google Play 批准符合政策的版本之前，用户可能无法进行任何应用内购买或使用应用内结算功能。
- 下架不会立即影响您的 Google Play 开发者帐号的信誉，但多次下架可能会导致您的 Google Play 开发者帐号被中止。

注意：在解决所有违反政策的行为之前，请勿尝试重新发布已下架的应用。

暂停

- 该应用（包括之前的所有版本）都会从 Google Play 中下架，用户将无法再下载该应用。
- 如果应用违规情节严重、屡次违反政策，或者多次遭到拒绝或下架，我们就可能会暂停该应用。
- 应用被暂停后，用户将无法查看该应用的商品详情。

- 您无法再使用已暂停应用的 APK 或 app bundle。
- 用户将无法在该应用中进行任何应用内购交易或使用任何内购结算功能。
- 应用被暂停视同于受到警示，会对您的 Google Play 开发者账号的信誉造成不利影响。多次收到警示可能会导致个人以及相关的 Google Play 开发者账号被终止。

公开范围受限

- 您的应用在 Google Play 上的曝光度受到限制。您的应用将继续在 Google Play 上架，并且用户可以直接访问该应用的商品详情链接。
- 将您的应用设置为“公开范围受限”状态不会影响您的 Google Play 开发者帐号的信誉。
- 将您的应用设置为“公开范围受限”状态不会影响用户查看应用的现有商品详情。

地区限制

- 只有特定地区的用户才能通过 Google Play 下载您的应用。
- 其他地区的用户将无法在 Play 商店中找到您的应用。
- 之前已安装应用的用户可以继续在其设备上使用应用，但不会再收到更新。
- 地区限制并不会影响您的 Google Play 开发者帐号的信誉。

帐号受限状态

- 如果您的开发者帐号处于受限状态，目录中的所有应用都将从 Google Play 下架，并且您将无法再发布新应用或重新发布现有应用。您仍可使用 Play 管理中心。
- 所有应用都下架后，用户将无法查看应用的商品详情和您的开发者资料。
- 现有用户将无法进行任何应用内购买或使用任何应用内结算功能。
- 您仍可使用 Play 管理中心，向 Google Play 提供更多信息，以及修改帐号信息。
- 解决所有违反政策的行为后，您将能重新发布应用。

终止帐号

- 如果您的开发者帐号遭到终止，目录中的所有应用都将从 Google Play 下架，并且您将无法再发布新应用。这也意味着，所有相关的 Google Play 开发者帐号也将被永久中止。
- 如果您的应用多次被暂停或因严重违反相关政策而被暂停，则还可能会导致您的 Play 管理中心帐号遭到终止。
- 由于已终止帐号中的应用会被下架，因此用户将无法查看应用的商品详情和您的开发者资料。
- 现有用户将无法进行任何应用内购买或使用任何应用内结算功能。

注意：如果您尝试开设一个新帐号，那么该新帐号也会被终止（不退还开发者注册费），因此请勿在您的任意帐号被终止时注册新的 Play 管理中心帐号。

休眠帐号

休眠账号是指处于闲置或弃用状态的开发者账号。休眠账号不符合《开发者分发协议》 规定的信誉良好条件。

Google Play 开发者账号旨在服务于那些发布和积极维护应用的活跃开发者。为防止滥用，我们会定期停用休眠、未使用或没有进行其他明显活动（例如发布和更新应用、查看统计信息或管理商品详情）的账号。

停用休眠账号会导致相应账号无法使用。您将无法再访问 Play 管理中心内的任何相关报告、统计信息、数据洞见或其他信息，除非您恢复使用休眠账号。注册费不予退款。在停用您的休眠账号前，我们会使用您为该账号提供的联系信息向您发送通知。

休眠账号被停用后，您日后仍可创建新账号并在 Google Play 上发布内容。

管理和举报政策违规行为

违规处置申诉

如果我们的处理存在误判，过后发现您的应用并未违反 Google Play 计划政策和开发者分发协议，我们将恢复您的应用。如果您已仔细阅读相关政策，并认为我们的决定可能有误，请按照违规处置电子邮件通知中的说明或点击此处对我们的决定提出申诉。

其他资源

如果您需要关于我们执行的违规处置措施或用户给出的评分/评论的更多信息，请参阅以下资源或通过 Google Play 帮助中心与我们联系。不过，我们无法为您提供法律咨询。如果您需要法律建议，请咨询法律顾问。

- 应用验证
- 举报违反政策的行为
- 针对帐号终止或应用下架问题与 Google Play 联系
- 一般警告
- 举报不当应用和评论
- 我的应用已从 Google Play 下架
- 了解有关终止 Google Play 开发者帐号的信息

Play 管理中心要求

为了保护我们生机蓬勃的应用生态系统，进而提供安全的使用体验，Google Play 要求所有开发者必须完成 Play 管理中心要求的事项，包括验证与 Play 管理中心开发者账号关联的个人资料。经过验证的信息将在 Google Play 上显示，以帮助用户建立对开发者的信任和信心。详细了解 Google Play 上显示的信息。

Google Play 提供两种类型的开发者账号：个人账号和组织账号。为了获得顺畅的新手入门体验，请务必选择正确的开发者账号类型，并完成必要的验证。详细了解如何选择开发者账号类型。

在创建 Play 管理中心账号时，提供以下服务的开发者必须以“组织”身份注册：

- 金融产品和服务，包括但不限于银行服务、贷款、股票交易、投资基金、加密货币软件钱包和加密货币交易。详细了解金融服务政策。
- 健康类应用，例如医疗应用和人体研究应用。详细了解健康类应用。
- 获准使用 VpnService 类的应用。详细了解 VPN 服务政策。
- 政府应用，包括由政府机构开发或代表政府机构开发的应用。

选择账号类型后，您必须：

- 准确提供您的开发者账号信息，其中包括以下详细信息：
  - 法定名称和地址
  - 邓氏编码 （如果以组织身份注册）
  - 联系电子邮件地址和电话号码
  - Google Play 上显示的开发者电子邮件地址和电话号码（如适用）
  - 付款方式（如适用）
  - 与您的开发者账号相关联的 Google 付款资料
- 如果是以组织身份注册，请确保您的开发者账号信息是最新的，并且与您的 Dun & Bradstreet 资料中存储的详细信息一致

在提交应用之前，您必须：

- 准确提供所有应用信息和元数据
- 上传应用的隐私权政策，并在“数据安全”部分填写需要披露的信息
- 提供有效的演示账号、登录信息，以及 Google Play 审核您的应用所需的所有其他资源（具体而言，包括登录凭据、二维码等）。

与以往一样，您必须确保您的应用提供稳定可靠、引人入胜且响应迅速的用户体验；仔细检查应用中的所有内容（包括广告联盟、分析服务和第三方 SDK），确保它们均符合 Google Play 开发者计划政策；如果您的应用的目标受众群体包括儿童，还要确保遵守我们的家庭政策。

切记，您务必要查看开发者分发协议和所有开发者计划政策，以确保您的应用完全符合要求。

Developer Distribution Agreement

需要更多帮助?

请尝试以下步骤：

与我们联系

向我们提供更多信息，以便我们帮您解决问题