

Google

从容顺应新的 广告环境

2022

Google 策略方案：打造高度
注重隐私的解决方案





概述

简介

用户对隐私的日益关注已经引发了一系列变化。在未来几年，这些变化将重塑数字广告生态系统。日益强烈的用户隐私保护期望、全球各地陆续出台的新法规以及浏览器和操作系统的近期变化皆表明，隐私至上的未来已近在眼前。

Google 重视发布商的成功以及他们在由广告资助打造的开放互联网中发挥的重要作用。我们会尽力支持各种规模的发布商从容顺应当今的隐私保护环境。

本策略方案概述了发布商可以使用的 Google 解决方案和策略。

本策略方案包含互动元素，可帮助您快速找到对您最重要的内容。您可以使用  且  跳转至您感兴趣的部分。

在整个策略方案中，您随时可以通过左上角的 **导航栏** 跳转至各个部分。

每个部分中链接到的  **更多资源** 可帮助您采取行动。

第一部分

为迎接高度注重隐私的未来做好准备 →

01. 为何隐私如此重要
02. 发布商面临什么风险
03. Google 的方法和愿景

第二部分

管理法规和用户意见 →

01. 监管环境
02. “隐私权和消息” 标签页
03. 支持发布商

第三部分

注重隐私的解决方案 →

01. Privacy Sandbox
02. 内容相关受众群体
03. 程序化直接交易
04. AdSense 搜索广告

第四部分

建立第一方受众群体 →

01. 定义第一方数据
02. 扩大受众群体
03. 利用受众群体变现
04. 供程序化交易使用的标识符

第五部分

适应各种应用平台变化 →

01. 平台变化
02. iOS 解决方案
03. Android 解决方案

第一部分

为高度注重隐私的 未来做好准备

概述

由于隐私保护环境飞速演变，当今的数字广告业务管理流程似乎比以往更复杂。所幸的是，发布商可通过一些方式来适应隐私保护趋势，从而发现新商机。

发布商可以测试新策略并改进各自的商业行为，在尊重客户隐私偏好的同时维持并增加收入。

- ➔ 01. 为何隐私如此重要
- ➔ 02. 发布商面临什么风险
- ➔ 03. Google 的方法和愿景

为何隐私如此重要

消费者观念转变

随着消费者的隐私权意识不断提高以及对数据隐私的期望发生转变，隐私保护已经成为很多用户最关心的问题。

(信息来源: [EY 全球消费者隐私权问卷调查](#))

2/3

[EY Boston Consulting Group 和 Google 联合开展的一项新研究](#)表明，尽管三分之二的消费者希望获得针对其兴趣定制的个性化广告，但近一半的消费者不愿为之共享个人信息。

监管响应呈增长之势

全球各地相继推出法规，强制推行数据方面的各种保护责任，以满足消费者对个人隐私保护的期望。

对于企业收集和使用消费者数据的方式，全球各地也在不断加强监管审查力度。鉴于大势如此，广告界已开始逐步淘汰用于开展营销和衡量相关指标的跨网站和跨设备标识符。



发布商面临什么风险

根据最近 [Deloitte](#) 针对美洲地区发布商开展的一项研究，90% 的受访者要么认为在线隐私改革已然姗姗来迟，要么认为恰逢其时。

100 亿
美元

随着行业趋势从使用第三方 Cookie 转向日益尊重客户隐私偏好，[McKinsey](#) 发布的一份报告预计，仅在美国，发布商的整体广告收入就将减少 100 亿美元。

近期的 [BCG](#) 隐私保护迫切性调研报告表明，在亚太地区，超过 60% 的受访公司认同隐私保护对其所在国家/地区的用户非常重要，超过 70% 的受访公司认同在隐私保护方面准备不充分将会导致严重后果。

80%

该报告提到，如果小型发布商有超过 80% 的广告收入来自以数据为依据的广告，他们最有可能受到收入下降的严重影响。

对发布商而言，收入损失意味着可用于制作新内容、经营业务和支付员工薪资的资金变少。

但若赢得上游用户的信任，也就能掌握一个大好商机。随着用户对您品牌的信任度不断提升，您可以使用的信息便会不断增加，这有助于您提升营销策略的相关性和有效性。

在转型的过程中，肯定会面临颇多风险。正因如此，发布商必须采取积极措施，为顺应新的广告环境做好准备。Google 正在大力投资开发全套解决方案，帮助发布商在隐私至上的未来维持收入。

Google 的方法和愿景

Google 支持由广告资助打造的开放互联网，同时也支持保护用户隐私。我们始终致力于维护一个蓬勃发展的生态系统，让全球范围内的用户都可以访问由广告资助打造的内容，并确信其隐私选择会受到尊重。

我们认为，与用户和第一方数据建立直接关系的发布商应当有能力通过更有助益的广告来自定义和改善用户体验。



Google 的方法和愿景

我们认为正确的原则

1

首先，我们认为用户隐私与个性化广告并不是互斥的。

我们可以营造一个蓬勃发展的互联网，发布者可以在其中制作内容，全球用户可以继续访问这些由广告资助打造的内容，同时确信其数据受到保护。

2

其次，与用户和第一方数据建立直接关系的发布者应当有能力自定义和改善用户的广告体验。

3

最后，在网站和应用中跟踪个人用户不是尊重用户隐私的做法。

我们认为此类解决方案并不符合用户所呼吁的变革的精神。

第二部分

管理法规和 用户意见

概述

Google 致力于推出各种工具来支持合作伙伴开展合规工作。继续阅读，详细了解有哪些可用的解决方案可帮助发布者驾驭日益复杂的监管广告环境。

- ➔ 01. 监管环境
- ➔ 02. “隐私权和消息” 标签页
- ➔ 03. 支持发布者

! 请注意：

Google 工具并不保证一定能符合法规要求。请咨询您的法律顾问，确定特定法规是否适用于您的业务，以及如果适用，那么我们的哪些工具（如果有）可以帮助您遵守法规。

Google 致力于帮助我们的合作伙伴在涉及我们产品的领域在全球范围内都达到合规要求

近期的一些重要示例：



AADC (适龄设计规范)

Google 提供多种解决方案来协助保护未成年人，包括 TFUA (用于表示用户未达到同意年龄的标记)



CCPA (加州消费者隐私法案)

推出受限的数据处理 (RDP)



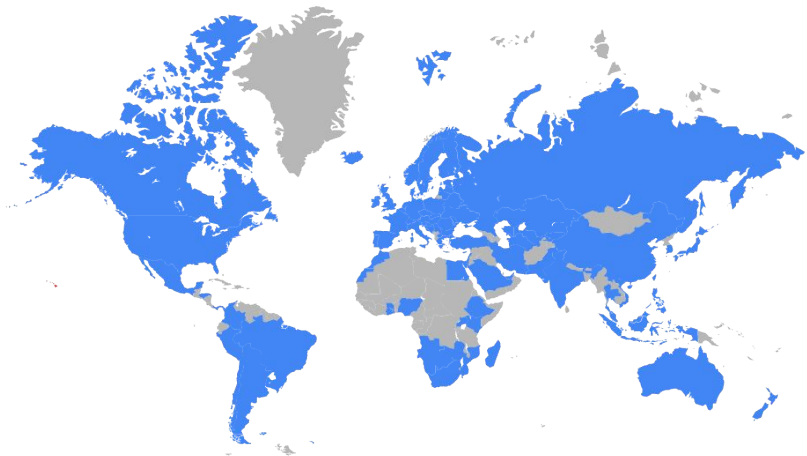
PIPL (个人信息保护法)

对于确定需要征求用户同意才能投放个性化广告的发布商，我们为其提供非个性化广告

除了上述近期示例，Google 长期以来一直为发布商提供 [各种工具来帮助其遵守 GDPR](#)。

全球陆续出台的各种法规在不断提高隐私保护标准

全球广告行业仍将继续面临越来越严苛的监管。对于发布商可以如何采取措施以更加充分地即将发生的变化做好准备，我们有多项建议：



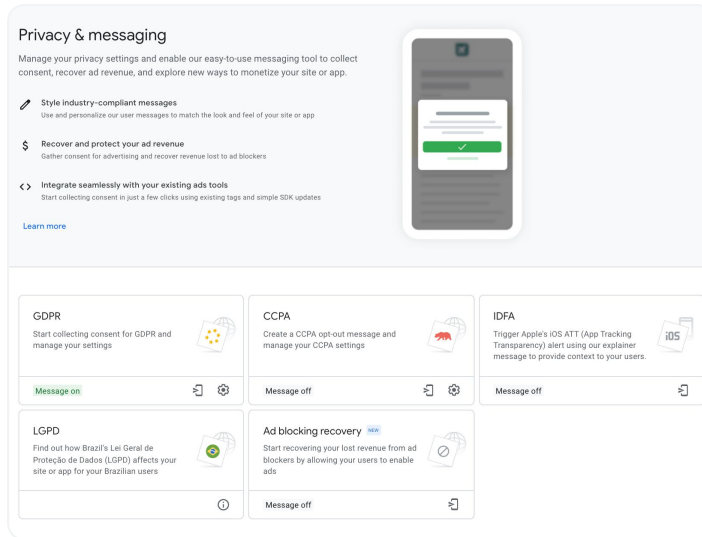
- ① **与您的法务团队合作，**
共同确保您的隐私权规范符合现行法律的要求，并力求更加深入地理解未来法规可能对您的国际业务产生哪些影响。
- ② **对数据收集和使用保持透明，**
并确保您的隐私权政策已是最新版本。让用户轻松了解您收集哪些信息、如何使用这些信息、可能与谁共享这些信息及其原因，以及用户允许您使用其信息将获得哪些价值。
- ③ 在适当情况下**实施意见征求管理平台 (CMP)，**
确保您的用户能够透明查看和控制其数据的使用情况。有特定需求的发布商可以选择构建自己的意见征求解决方案，但发布商和开发者通常可以利用 CMP 更轻松地收集和管理网站和应用访问者的意见。通过这种方式，他们可以投放个性化广告，提供更出色的用户体验，并继续利用其数字内容变现。

“隐私权和消息” 标签页简介

为了帮助您更加深入地理解不同的隐私法规可能会对您的业务产生什么影响，“隐私权和消息” 标签页为您提供了一个集中位置，便于您及时了解相关法规和可以采取的措施，还可以选择向用户发送消息，从而驾驭广告环境并缓解业务受到的影响。只需点击卡片即可获取以下信息：

- 法规可能对您产生什么影响
- 如何为用户提供充分的控制权
- 其他 Google 资源，例如网站和开发者文档

目前，“隐私权和消息” 标签页分别针对 GDPR 和 CCPA（仅限网站）提供了可选的用户意见征求消息和拒绝消息。

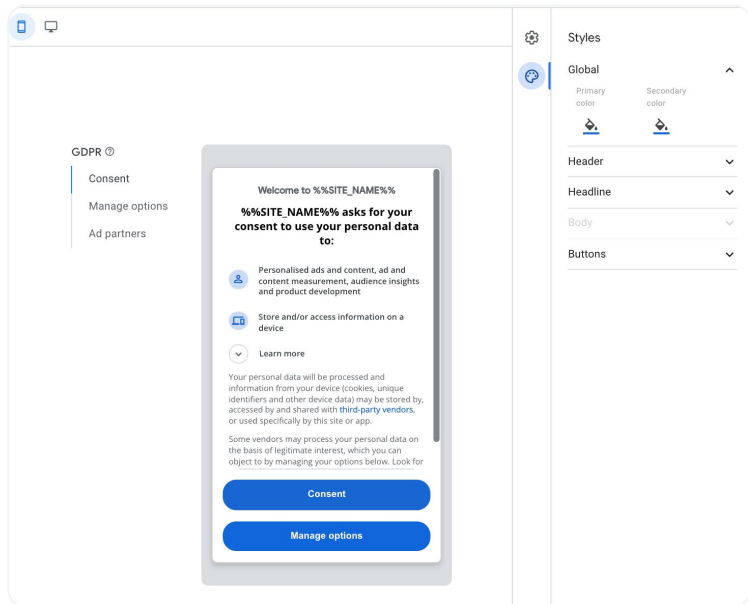


隐私权和消息 | 设置 GDPR 消息

借助“隐私权和消息”标签页中的可选消息功能，您可以创建并向用户显示消息，以帮助依据《一般数据保护条例》(GDPR) 收集所需要的同意。您通过“隐私权和消息”工具创建的消息会列出您的网站或应用使用的广告技术提供商，并会请求用户同意这些提供商将个人数据用于展示个性化广告和其他目的。此外，您还可以就您的网站或应用使用数据征得用户同意。

GDPR 消息包含多个“屏幕”（或“页面”），并根据用户在您的消息中点击的按钮和链接来显示具体的“屏幕”（或“页面”）。向用户显示的按钮选项取决于您在创建消息期间在“用户意见征求选项”部分中的具体选择。

有关配置和部署 GDPR 消息的更多信息，请参阅以下帮助中心文章：[Ad Manager](#)、[AdSense](#) 和 [AdMob](#)。



Google 产品

Ad Manager

Ad Manager 360

AdMob

AdSense



平台

应用

网站



需求类型

间接

直接

请注意，Google 工具并不保证一定能符合法规要求。

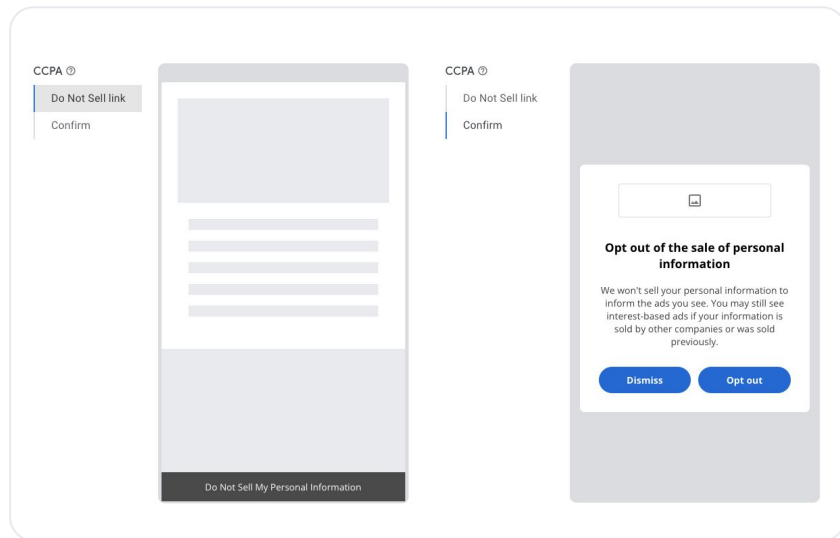
隐私权和消息 | 设置 CCPA 消息

CCPA 第 999.306 条规定，发布商必须发布“个人信息拒售权利声明”(Notice of Right to Opt-Out of Sale of Personal Information)。CCPA 消息会面向美国加利福尼亚州境内的用户显示，为他们提供选择拒售个人信息的机会。

一条 CCPA 消息会包含多个“屏幕”(或“页面”)，以向查看相应消息的用户显示。

CCPA 消息中有以下元素：

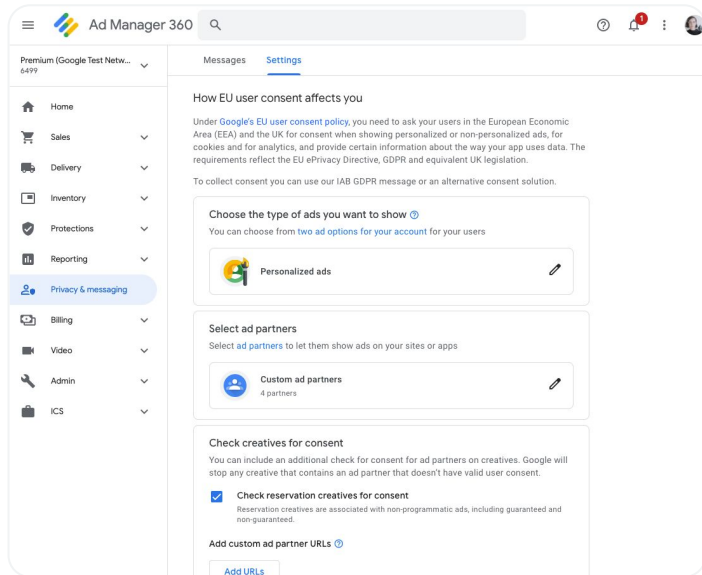
- **“不出售”链接**：指向您的 CCPA 消息的链接，会按照您所选的格式和设置显示“不出售我的个人信息”链接。当用户点击该链接后，系统即会打开“确认”页面并在其中显示“不出售个人信息”对话框。
- **“确认”页面**：您的 CCPA 消息的确认页，会显示“不出售个人信息”对话框。用户点击相应按钮即可确认他们的决定。



用户自主选择环境下的变现

为了帮助发布商遵守 GDPR、CCPA 和其他相关法规，Google 提供了多种解决方案来协助投放去个性化广告。这些解决方案包括非个性化广告、受限广告和受限的数据处理。

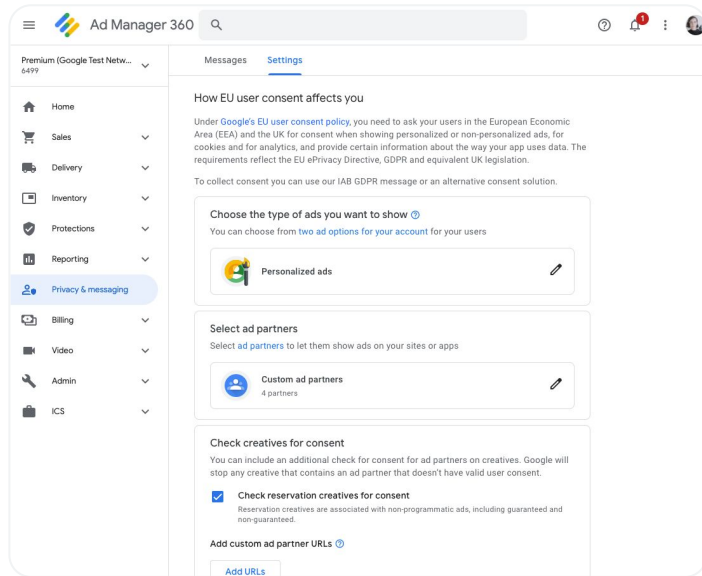
- **非个性化广告**：非个性化广告是指使用情境信息来定位的广告，而并非根据用户过去的行为投放的广告。Google 会禁止所有 [基于兴趣的受众群体定位](#)，其中包括受众特征定位和用户列表定位。
- **受限的数据处理**：当您启用 [受限的数据处理](#) 后，Google 会限制其使用数据的方式，并且仅会向受 CCPA 监管的加利福尼亚用户投放非个性化广告。
- **受限广告**：借助 [受限广告](#)，发布商即使未就 Cookie 或其他本地标识符征得用户同意，也能通过一种受限的方式投放广告。发布商使用 IAB 透明度和用户意见征求框架 (TCF) v2.0 时，如果未就用途 1 征得用户同意，我们会尝试投放符合条件的受限广告。



广告技术提供商控件

Ad Manager 为发布商提供了一些控件，用于在面向欧洲经济区 (EEA) 和英国的用户时，选择允许使用哪些 [广告技术提供商 \(ATP\)](#) 的广告投放和衡量技术来支持广告投放、效果衡量及其他功能。该 ATP 列表适用于程序化广告素材需求，并可扩展到预订型广告素材需求。

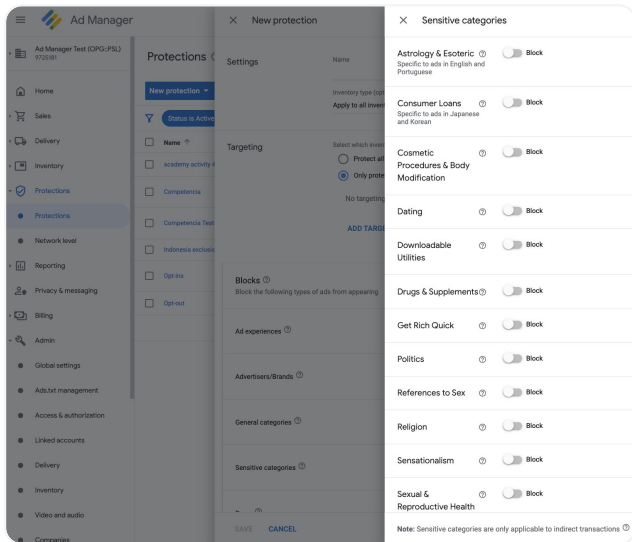
- **预订级控件：** 预订型广告素材会与非程序化订单项相关联，包括有保证的订单项（包天订单项和包量订单项）和无保证的订单项（联盟订单项、批量订单项、价格优先订单项和自家订单项）。在确定预订型广告素材是否符合投放条件时，Google 会检查您是否已就自己声明的所有广告技术提供商征得用户同意。
- **实时出价 (RTB) 广告素材检查：** 选择启用 RTB 广告素材检查后，Google 可以在 Ad Manager 中审核您的 RTB 广告素材，以过滤掉（我们的系统检测到）供应商像素未包含正确用户意见征求的 RTB 广告素材。



保护未成年人

为了帮助发布商遵守 COPPA、AADC、COADP 和其他保护未成年人的法规，Google 提供了多种解决方案来协助投放去个性化广告和过滤广告素材。我们的解决方案包括**面向儿童的内容标记**（☞ [TFCD](#)）、**用于表示用户未达到同意年龄的标记**（☞ [TFUA](#)）和 **广告内容控件**。

- **TFCD**：将您的广告请求标记为面向儿童的内容，其中包括广告去个性化和广告素材过滤。该功能旨在帮助您遵守美国《儿童在线隐私保护法》(COPPA)。
- **TFUA**：对广告请求进行标记，以确保针对欧洲经济区 (EEA)、英国和瑞士未达到同意年龄的用户采用“受限的数据处理”模式。这项功能旨在帮助您遵守《一般数据保护条例》(GDPR) 和相关的儿童隐私保护法规，例如《适龄设计规范》(AADC)。
- **广告内容控件**：广告内容规则可以帮助您控制哪些类型的广告客户类别符合媒体资源的投放条件。具体而言，您可以使用这些规则来控制面向未满 18 周岁用户的内容的广告体验。



第三部分

注重隐私的 解决方案



概述

我们的目标是提供持久的解决方案，让您轻松实现业务目标，同时确保尊重用户隐私偏好。以下列出了我们建议发布商采用的一些方法：

- ➔ 01. Privacy Sandbox
- ➔ 02. 内容相关受众群体
- ➔ 03. 程序化直接交易
- ➔ 04. AdSense 搜索广告

了解 Privacy Sandbox

创建更私密的互联网

Privacy Sandbox 计划旨在开发能够实现以下目标的网络技术：保护用户在线隐私，同时为公司和开发者提供助力其发展数字业务的工具。Privacy Sandbox 可减少跨站点和跨应用跟踪，同时帮助向所有用户免费开放在线内容和服务。



构建新技术以保持信息私密性

用户应当能够享受其浏览和应用体验，而不必担心哪些人收集了哪些个人信息。Privacy Sandbox 技术旨在使当前的跟踪机制失效，并阻止隐蔽跟踪技术，例如指纹识别。



使发布商和开发者能够免费提供在线内容

全球数十亿用户每天都要访问网站和应用上的信息。为了在不借助侵入式跟踪的情况下提供这种免费资源，发布商和开发人员需要利用隐私保护替代方案来满足其关键业务需求，包括提供相关内容和广告。



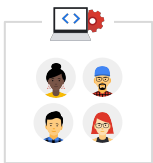
与业界合作制定新的互联网隐私保护标准

互联网是全球经济增长的信息来源和引擎。Google 诚挚邀请行业成员（包括发布商、开发者、广告客户等）共同参与，为制定更好的 Web 和 Android 隐私标准做出贡献。

Privacy Sandbox for the Web

Privacy Sandbox for the Web 使用最新的隐私技术（如差分隐私、k-匿名性和设备端处理）来实现过去由第三方 Cookie 支持的功能。Privacy Sandbox 还有助于限制站点可以获取的信息量，从而帮助限制指纹识别等其他形式的跟踪，让您的信息保持私密、安全和可靠。

针对用户兴趣 主题



允许广告客户根据展示特定兴趣的主题（由浏览器定义）来展示相关广告。

再营销 FLEDGE



在设备竞价中选择最相关的广告，包括基于用户浏览记录的再营销广告。

衡量 归因报告



支持各种关键广告客户衡量用例，从事件级到聚合级报告一应俱全。



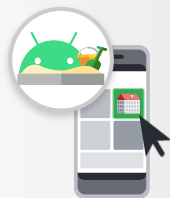
Privacy Sandbox on Android

2022 年 2 月 16 日，Google 宣布将 Privacy Sandbox 计划扩展至 Android。Android 致力于从根本上增强移动应用生态系统的隐私保护，同时支持关键广告用例，并让用户能够访问其喜爱的应用。

Web 和移动应用依赖于完全不同的技术，但广告支持 Web 生态系统的方式与支持应用生态系统的方式有相似之处。

这些技术的开发、测试和采用预计至少需要两年时间。在此过程中，Android 将共享更多详细信息。

Google 的广告团队全力支持 Android 的愿景，并且将与 Android 和应用生态系统携手合作，提供关于打造持久隐私安全解决方案的反馈，继续让广告成为支持和发展其业务的有效方式。



参与 Privacy Sandbox

在许多情况下，发布者不需要直接采用 Privacy Sandbox 中的隐私保护技术，因为其广告技术提供商可能会代为实施这些解决方案。



获取最新信息

访问 [Privacy Sandbox](#) 网站，了解有关 [Web](#) 和 [Android](#) 的当前提案的更多信息。



提供反馈

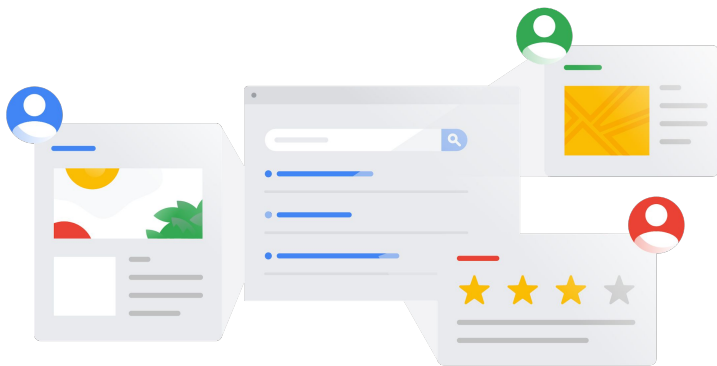
直接向 [Chrome](#) 和 [Android](#) 团队提供反馈，以帮助创建 API 提案。



内容相关数据有助于让广告客户触达感兴趣的受众群体

发布商为广告客户创建令人信服的以隐私为中心的受众群体列表时，最常使用且最易于实现的一种方式是使用内容相关数据。在实践中，这非常简单。例如，当您将文章或视频归类为与“个人健身”相关的内容时，可以放心地认为希望触达健身爱好者的广告客户会对在该内容上投放广告感兴趣。

从表面上看，这种方式很简单直接，但经验丰富的发布商要投入大量时间，为其内容相关信号添加额外的颗粒度，而这又有助于增加价值，并为其广告资源创造更多机会。在以上示例中，如果您为“瑜伽”、“骑行”或“跑步”等“个人健身”内容创建额外的子类别，则广告客户可以进一步创建个性化信息，并且您可以针对更具体的受众群体收取更高的 CPM。



使用键值对执行内容相关定位策略

您可以将键值对作为额外参数添加到广告请求中，以便于指定定位条件。键值对可以帮助您的广告客户和买方覆盖他们的目标受众群体或目标人群，并在协商广告系列时为您提供广告资源增值。

🔗 完整指南

如要开始使用键值对，请遵循以下步骤：

- ① 制定一个关于如何以最佳方式使用键值对的方案
- ② 根据您的方案在您的广告资源网中添加新的键值对
- ③ 为网页或应用添加代码时，在 Google 发布商代码 (GPT) 中添加键值对
- ④ 在订单项、提案订单项以及其他部分中定位键值对



Google 产品

Ad Manager

Ad Manager 360



平台

应用

网站



需求类型

程序化*

直接

*仅适用于程序化直接交易

程序化直接交易

在当前高度注重隐私的环境中，程序化直接交易可以帮助发布商利用内容相关信号和第一方数据提高其广告资源的价值。

借助程序化直接交易，建立值得信任的一对一关系

借助 Ad Manager 中的有保证的程序化交易和首选交易广告系列，程序化直接交易功能可自动完成直销广告资源的协商和销售。

有保证的程序化：您和买方协商为买方预留的（有保证）广告资源的价格和条款。按协商的价格指定的广告资源仅适用于相应买方。

首选交易：您和买方协商广告资源的价格和条款，买方可视需要购买。如果有针对相应广告资源的广告请求，买方有机会率先或优先按照协商好的价格进行出价。

程序化直接交易扩展了程序化广告的承诺，让广告客户和发布商能够比以往更加轻松地实施直接预订式购买，从而为广告客户和发布商创造更多价值。



Google 产品

Ad Manager

Ad Manager 360



平台

应用

网站

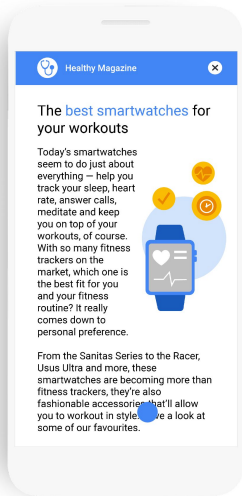


需求类型

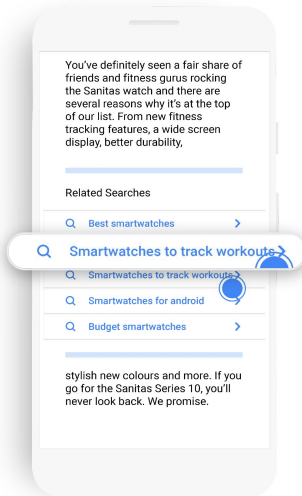
程序化

AdSense 搜索广告

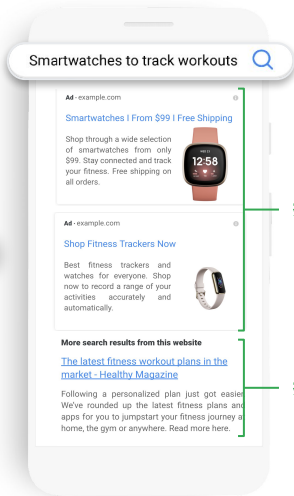
即使没有个性化，搜索广告的效果也非常好。AdSense 搜索广告 (AFS) 以关键字而非用户为目标。



1. 用户访问网站上的文章



2. 用户点击相关搜索单元中的搜索字词以探索更多内容。



3. 用户查看相关搜索广告和搜索结果。

- 借助内容页面上的相关搜索实现多样化的广告收入**
 相关搜索可以帮助您的用户探索网站上的更多内容，并让您无需广告个性化即可实现多样化的广告收入。
- 通过搜索结果页变现以增加收入**
 AdSense 搜索广告 (AFS) 使用用户的搜索查询来投放针对性强且相关性高的广告。
- 效果出众的搜索广告**
 搜索广告、购物广告和其他富有视觉吸引力的广告格式在搜索页面上效果出众。AdSense 搜索广告 (AFS) 可允许您访问搜索广告预算。



Google 产品

AdSense 搜索广告



平台

应用

网站



需求类型

程序化

搜索广告仍然需要使用 Cookie 并就使用 Cookie 征得用户同意。

第四部分

建立第一方 受众群体

概述

Google 正在投资开发多种解决方案，让发布者更加轻松地收集、衡量和激活第一方数据。详细了解第一方数据可以如何帮助您为用户和买方增加价值。

- ➔ 01. 定义第一方数据
- ➔ 02. 扩大受众群体
- ➔ 03. 利用受众群体变现
- ➔ 04. 供程序化交易使用的标识符

定义第一方数据

“第一方”是指两方之间的直接一对一关系。第一方数据是指，您通过与访问您的网站或应用并为之互动的用户建立直接关系所获知的信息。

您可以从访问者处获知各种类型的信息，例如，某用户在注册简报时提供的电子邮件地址，或者也可以是某用户访问了您网站上的哪些页面。

即使在用户期望和法规不断变化的环境中，发布者仍然需要了解其受众群体是哪些人，为用户创造更多价值，并以富有创意且极具价值的方式为广告客户打包广告资源。随着用户继续采用不同的方式来与发布者内容互动、消费发布者内容并为其付费，建立有意义的关系的机会空前增多。

为用户增加价值以创建第一方数据

当您的受众群体允许您使用其数据时，他们希望获得一些回报。通过增强用户体验来建立公平的价值交换对于发展更深层次的用户关系至关重要。大多数发布者为其用户提供的主要价值是趣味性、信息丰富或实用性的原创内容。发布者可以通过多种方式将用户与其内容联系在一起——同时构建其第一方受众群体数据。



定义第一方数据

第一方数据与第三方数据的区别

广告行业正在加大对高度注重隐私的第一方数据的投资，并且逐渐弃用第三方数据。两者之间的主要区别如下：



数据由谁收集

第一方数据由网站或应用所有者收集和存储。第三方数据通常由专业数据收集企业在多个不属于其自身的网站上收集。



权限

对于第一方数据，用户向与其建立直接关系的企业提供使用其数据的许可，而企业将负责以合规方式使用数据。相比之下，第三方数据的收集和使用通常不会让用户全面知晓其数据是如何被激活的。

相关隐私法规对第一方数据和第三方数据都适用。因此，制定明确的隐私权政策非常重要，只有这样才能让用户确切知晓自己共享了哪些数据及其预期用途。

扩大受众群体



70% 的发布商认为其激活第一方数据的能力将在以隐私为中心的生态系统中提供显著优势。

[了解调研详情](#)

信息来源：Deloitte 研究 — 通过第一方数据实现面向未来的广告销售增长

大多数发布商（即使是规模较小的发布商）都可以轻松实施策略来扩充其第一方数据。许多发布商鼓励消费者登录以换取额外的内容或功能。

一些发布商甚至创建或收购全新的业务（例如忠诚度计划、信用卡服务或网店）以填补其数据空白。



案例研究

了解《华尔街日报》如何激活第一方数据以实现所需效果。

[了解详情](#)

利用受众群体变现

通过 PPID 使用您自己的第一方标识符

拥有现有第一方数据集的 Google Ad Manager 发布商可以使用 [发布商提供的标识符](#) (PPID) 创建加密标识符、构建受众群体并将广告投放到第一方细分受众群。PPID 由您设置和控制，即使第三方 Cookie 等第三方标识符不再受支持，PPID 也会继续正常运行。

发布商提供的标识符 (PPID) 是一种高度注重隐私的解决方案，因为它们具备以下特性：

- 必须经过哈希处理，并且 Google 无法访问底层数据。只有您本人知道它们的含义。
- 不得包含个人身份信息 (PII)。
- 特定于各个 Ad Manager 广告资源网，不与其他发布商共享，也不与任何其他标识符相联接。

案例研究

了解 Pandora 如何成功利用第一方数据变现。

[了解详情](#)

在考虑开发 PPID 时，请牢记以下步骤：

- ① 确定您有哪些可用的第一方数据。
 - 拥有用户登录数据的发布商能够基于此类用户数据开发 PPID。示例包括用户名和用户 ID。
 - 对于没有用户登录数据的发布商，也可以使用基于用户访问进行部署的发布商第一方 Cookie 来开发 PPID。它们可以基于各种属性，例如访问频率、访问的内容和结账购物车活动。
- ② PPID 会随每个广告请求一起传递给 Ad Manager，这将使用您现有的 GPT 代码、GMA SDK 或 IMA SDK。请与您的 Google 客户经理联系，了解激活事宜。



Google 产品

Ad Manager 360



平台

应用

网站



需求类型

直接

利用受众群体变现

使用受众群体解决方案构建和管理第一方细分受众群

PPID 可用于在 Ad Manager 360 受众群体解决方案中创建和管理第一方细分受众群。

当基于 PPID 的受众群体名单出现在 Ad Manager 360 受众群体解决方案中时，预订和程序化交易订单项随即可以定位到这些第一方受众群体，从而提高广告客户的广告效果和对于用户的广告相关性。然后，可以将各个 PPID 与每个广告请求一起传递到 Ad Manager 360，供 Ad Manager 360 用于与出现的任何第一方受众群体名单进行核对。

这样一来，若要允许将给定广告请求与基于 PPID 的受众群体名单相匹配，PPID 将成为一项关键因素。

此外，Ad Manager 360 还将 PPID 用于由您控制的核心广告服务器功能，包括：

- 预订的频次上限
- 预订的依序广告轮播
- 预订的广告素材轮播



发布者提供的信号

使用发布者提供的信号 (PPS) 进行情境信号传递以及传达第一方属性

发布者提供的信号 (PPS) 是一项新功能，目前处于 Beta 版阶段，可帮助您提高程序化变现能力。借助 PPS，发布者将能够使用标准化类目将其第一方受众群体属性和情境数据传达给程序化买方。

我们正在与合作伙伴合作，将业界标准纳入发布者提供的信号中。首先，我们将整合 IAB Tech Lab 的“卖方定义的受众群体”。

如要开始使用发布者提供的信号 (PPS)，请遵循以下步骤：

- 发布者或其 DMP/数据供应商合作伙伴将其受众群体细分为同类群组，并使用支持的标准化类目进行分类
- 发布者在出价请求中包含类目类别（如受众特征数据、兴趣或购买意愿）和/或细分 ID
- 买方读取类别/细分 ID 并决定是否出价。



Google 产品

Ad Manager

Ad Manager 360



平台

应用

网站



需求类型

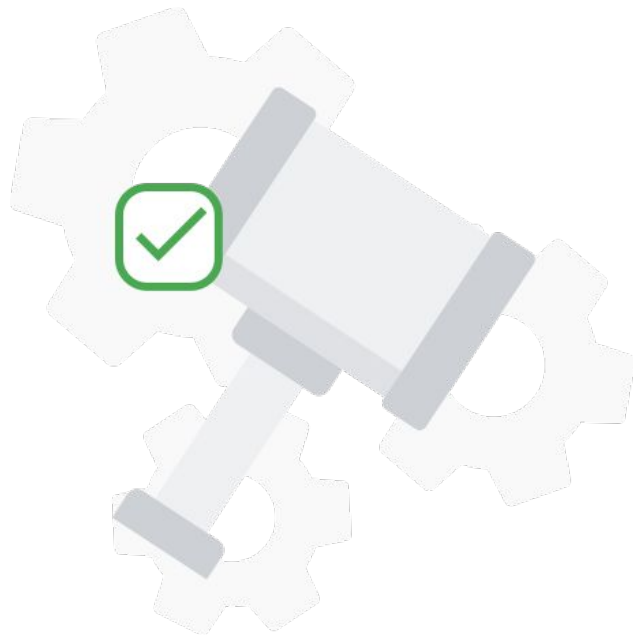
程序化

程序化直接交易

供程序化交易使用的标识符

在程序化销售广告资源时，标识符也非常重要。程序化出价方（即 DSP）实时接收出价请求，评估广告展示机会，并相应地出价。当第三方 Cookie 或 ID 被阻止或限制时，买方设置的频次上限功能会受到影响，这可能会导致用户重复看到相同的广告。因此，如果没有标识符，某些广告客户可能会决定完全排除特定媒体，而且发布商的收入可能会有所降低。

此外，利用程序化出价请求中出现的标识符，出价方可以根据随着时间推移用户反复触及及发布商提供的相同标识符而逐渐了解用户的兴趣。这些信息可用于在发布商的网站/应用上向用户投放更加个性化的广告，从而改善广告效果和用户体验。

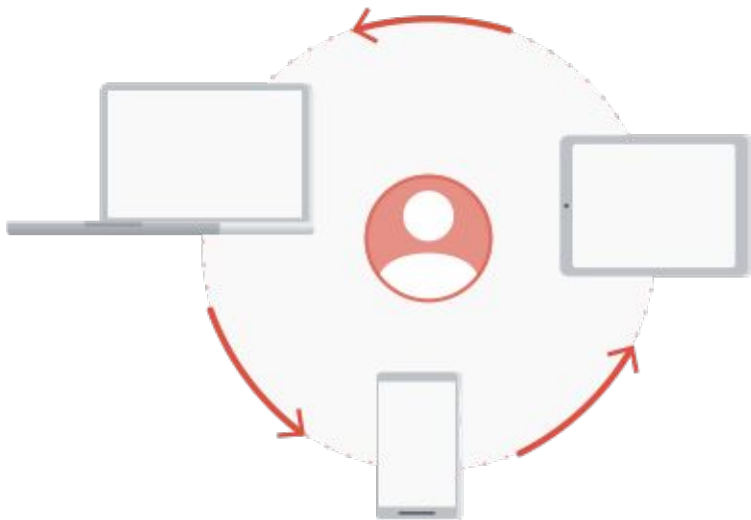


供程序化交易使用的 PPID

当您在 Ad Manager 360 界面中启用供程序化交易使用的 PPID 时，如果第三方 Cookie 或设备 ID 不可用，Google 的程序化广告需求可以利用给定广告请求中的 PPID 来支持对您的程序化流量设置买方频次上限和基于兴趣的广告个性化。

请务必注意，在与 Google 需求共享 PPID 之前，Ad Manager 会将 PPID 转换为按发布商分类的 ID，这样就无法在其他发布商的网站和应用中识别用户。从您的 Ad Manager 广告资源网共享的 PPID 绝不会与从其他 Ad Manager 广告资源网共享的 PPID 相匹配，这会将 ID 的使用限制在同一个 Ad Manager 广告资源网中。

总之，在与 Google 程序化需求共享您的 PPID 时，买方频次上限和基于兴趣的广告个性化仅可用于通知对您广告资源的出价，这有望增加您的程序化收入，并改善广告效果和用户体验。



发布商第一方 Cookie

使用发布商第一方 Cookie 为各种规模的发布商启用第一方标识符

当第三方标识符无法在网站上使用时，仍可利用发布商第一方 Cookie 用于广告投放功能，例如对程序化流量设置频次上限和广告个性化。

借助发布商第一方 Cookie，Google 可以利用用户在特定发布商网站上进行广告互动的相关信息来提高同一网站上的广告相关性。

什么是发布商第一方 Cookie？

- Google 代表您设置的第一方 Cookie
- 隐私优先，以您的网站为范围，不与其他发布商共享，也不与任何其他标识符相联接
- 提供了可选控件，发布商可以通过控件禁止使用发布商第一方 Cookie 来实现程序化广告个性化



Google 产品

Ad Manager

AdSense



平台

网站



需求类型

程序化*

*仅适用于 DV360 和 Google Ads，有关适用于 Authorized Buyers 用户和公开出价方的解决方案，请参阅 [安全信号](#) 幻灯片

自动第一方标识符

使用同应用标识键为各种规模的发布者启用第一方标识符

当移动广告 ID 不可用时，同应用标识键支持用一种顺畅、有效且隐私优先的方式来投放个性化广告。

同应用标识键可以利用从您的应用收集的数据（例如用户在您的应用内进行的广告互动的相关信息）来提高广告相关性，让您无需在各个第三方应用中跟踪用户，即可在 iOS 平台上投放切实相关的广告。

什么是同应用标识键？

- 第一方 ID 由 Google 在您的应用上设置
- 隐私优先，以您的应用为范围，不与其他发布者共享，也不与任何其他标识符相联接
- 提供了可选控件，供发布者禁止使用同应用标识键来实现程序化广告个性化



Google 产品

现已推出：

AdMob

即将推出：

Ad Manager



平台

应用



需求类型

程序化*

*仅适用于 DV360 和 Google Ads，有关适用于 Authorized Buyers 用户和公开出价方的解决方案，请参阅 [“安全信号”幻灯片](#)

安全信号

尊重与安全信号的直接关系

我们正在打造一项功能，使发布商能够通过 Ad Manager 与 Authorized Buyers 用户和公开出价方安全地共享信号。Google 将无法读取通过我们系统传递的信号，从而保护发布商与买方之间关系的机密性。



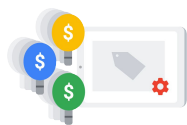
1. 发布商实施 ID Provider 解决方案并将相关代码添加至其网站



2. 在 Ad Manager 界面中，发布商支持所选合作伙伴收集传递至 Ad Manager 的信号



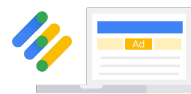
3. 用户访问发布商网站



4. Ad Manager 将安全信号从发布商路由至发布商在出价请求过程中合作的出价方



5. 出价方将出价响应发送回 Ad Manager，同时考虑安全信号



6. Ad Manager 选择获胜候选人并展示广告



Google 产品

Ad Manager

Ad Manager 360

AdMob



平台

应用

网站



需求类型

程序化*

*仅适用于 Authorized Buyers 用户和公开出价方。不适用于 DV360 或 Google Ads。

第五部分

适应各种应用 平台变化

概述

Google 的隐私保护方法扩展至所有平台和设备。尽管近年来网络隐私受到了极大的关注，但对于发布商来说，了解当前的应用格局并为未来做好准备是非常重要的。

- ➔ 01. 平台变化
- ➔ 02. iOS 解决方案
- ➔ 03. Android 解决方案

平台变化

技术变革从根本上改变了数字广告行业的基础

用户期望不断提升，这不仅促使出台更多法规，还导致技术变更，从而限制使用用户标识符：

- 对于企业收集和使用消费者数据的方式，全球各地也在不断加强监管审查力度。移动操作系统正在限制第三方 Cookie 和移动广告标识符，从而摆脱跨网站跟踪用户的机制。不断变化的格局正在逐步淘汰用于营销和衡量的跨网站和应用标识符。
- 与此同时，移动操作系统等技术平台已宣布或实施新政策来改变收集、共享和衡量用户数据的方式。

推出广告标识符 (IDFA) 和广告 ID

2012-2013

Apple 宣布对 IDFA 加以限制

2020

Apple 执行新的限制

2021

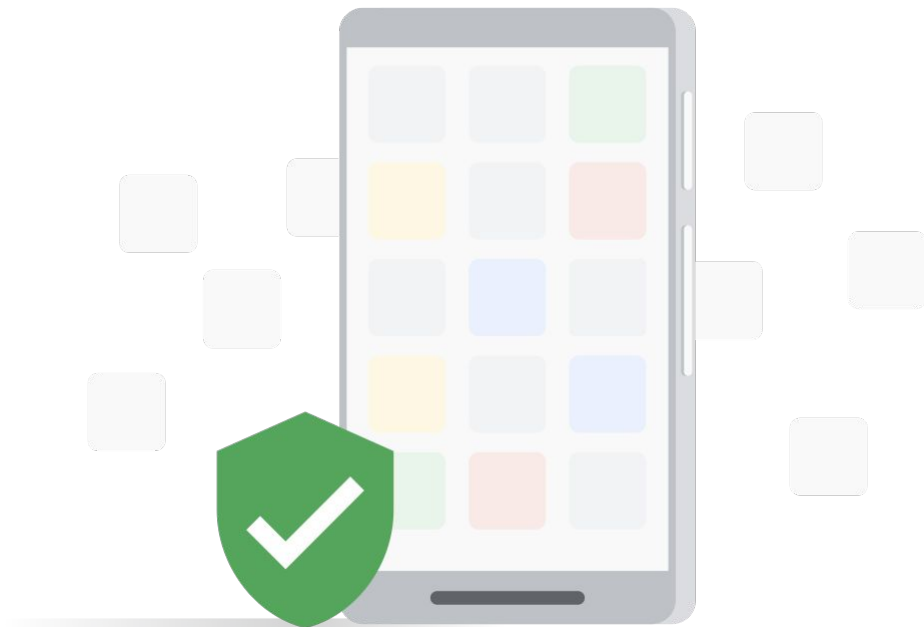
Android 宣布将 Privacy Sandbox 扩展至应用

2022

iOS 解决方案

2020 年 6 月，Apple 宣布对 iOS 14 进行一项更新，要求应用必须先通过一种称作“应用跟踪透明度”(ATT) 框架的提示征得用户许可，才能访问 Apple 的广告客户标识符 (IDFA)。

- 这些变更会导致您无法充分了解表明广告促成转化的情况的关键指标，并会影响广告客户对广告展示机会的估价和出价。
- 因此，应用发布商已经看到其 iOS 上的 Google 广告收入受到了重大影响。
- 请继续阅读，了解关于如何为 iOS 14+ 更新您的应用并帮助保护您的广告收入的建议。



iOS 解决方案



始终保持您的 SDK 为最新版本

始终保持您的 GMA SDK 为最新版本以利用最新的特性和功能，包括 SDK 实例 ID 和同应用标识键。 ([↔ AdMob](#) ↔ [Ad Manager](#))



ATT 消息

确定 ATT 是否适合您的应用。Google 的 [↔ “隐私权和消息” 标签页](#) 提供了创建和管理 ATT 提示和可选铺垫消息的选项



Apple 的 SKAdNetwork

为了让广告客户将您的应用识别为有价值的广告流量来源，您需要使用 Google 的广告联盟键来配置 SKAdNetwork。 ([↔ AdMob](#) ↔ [Ad Manager](#))



中介组

对于 iOS 应用，您现在可以为广告请求（无论是否带有广告客户标识符 (IDFA)）创建不同的中介组。 ([↔ AdMob](#) ↔ [Ad Manager](#))



Google 产品

Ad Manager

Ad Manager 360

AdMob

AdSense



平台

应用



需求类型

程序化

直接

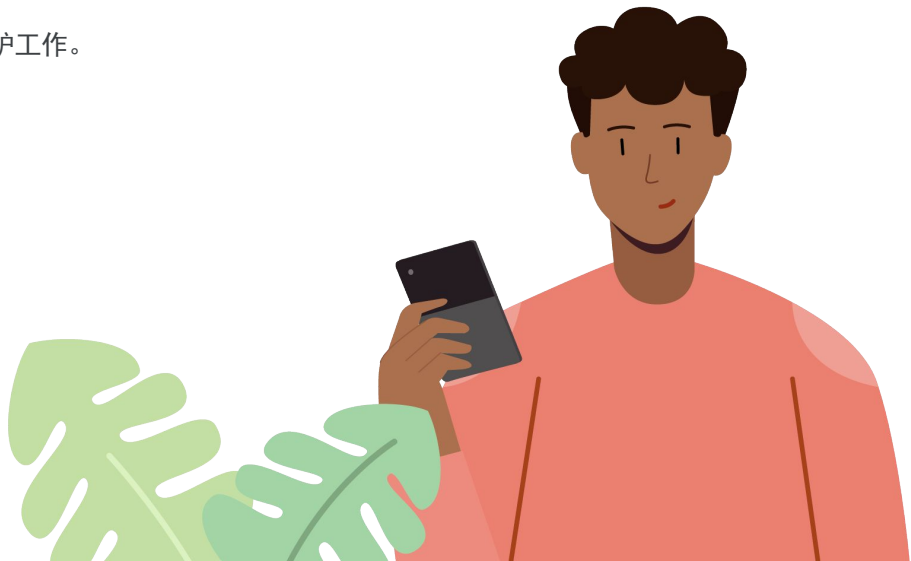
Android 解决方案

2021年7月，[Google Play 和 Android](#) 宣布了[政策更新](#)以加强隐私和安全性，让 Google Play 为开发者和消费者提供更安全、更值得信赖的体验。

2022年2月，Android 宣布推出 [Privacy Sandbox on Android](#)，这是一项行业多年通力合作的成果，旨在从根本上增强生态系统的隐私保护力度，同时未影响关键广告功能，也不会致使访问由广告资助打造的应用面临风险。

本部分旨在帮助您了解 Android 上发生的近期和长期隐私保护工作。

就像整个行业一样，Google Ads 将花费时间来评估提案并测试我们如何将这些解决方案整合到我们自己的产品中。因此，尽管您今天无需采取任何行动，但我们鼓励您熟悉 Android 正在采取的高级方法，如果您有兴趣，请在 [developer.android.com](#) 上注册了解最新动态。



Android 解决方案

2021 年，[Google Play](#) 和 Android 宣布推出几项新的政策更新和技术变更以增强隐私和安全性。

Android 更新

在 Google Play 管理中心中推出[Google Play](#) [“数据安全”](#) 部分，并需要在 2022 年第二季度之前在提交的新应用和更新中包括数据披露信息。

更新[Google Play](#) [家庭政策要求](#)。如果目标受众群体包含儿童，应用便不得传输儿童或年龄不明用户的某些标识符（包括广告 ID）。

我们将于 [2021 年底对 Google Play 服务做出更新](#)，其中包括：当用户在 Android 设置中选择停用借助广告 ID 实现的个性化广告时，系统将移除相应广告 ID。

[应用组 ID](#) 的开发者预览版，适用于分析或欺诈预防等基本用例。

建议采取的行动

请参阅 GMA SDK ([Google AdMob](#)) [Ad Manager](#) 和 [IMA SDK](#) 指南以更新 Play 管理中心信息。

拥有以儿童为受众群体的应用的开发人员应更新 SDK 以支持更新的 TFCD 和 TFUA 行为。

鼓励目前直接将广告 ID 用于基本非广告用例的开发人员采用应用组 ID（更多信息见下文）。

面向 Android 13 的应用需要在 AndroidManifest.xml 文件中声明 [Google Play 服务权限](#) 才能使用广告 ID。

面向 Android 13 的开发人员应更新其 SDK 或手动更新其清单。

为了保留用户选择停用广告 ID 的欺诈预防或分析等用例，开发人员应采用更新的 SDK 来支持应用组 ID。

将 Privacy Sandbox 计划扩展至 Android

2022 年 2 月 16 日，[Google 宣布](#)将 Privacy Sandbox 计划扩展至 Android。

Android 旨在从根本上增强移动应用生态系统的隐私保护，同时支持关键广告用例，并让用户能够访问其喜爱的应用。

Android 的方法

面向广告用例的新解决方案



不依赖跨多方标识符并限制用户数据共享的隐私保护 API。

减少隐蔽跟踪



可降低未公开数据收集可能性的技术。

与业界密切合作



通过参与和反馈来塑造可改善用户隐私并支持生态系统的设计。

这将是多年合作的成果

要点总结



01. 期待并适应广告环境的未来变化
02. 立即开始为未来做准备
03. 制定全面的方案和隐私策略
04. 与法务团队及合作伙伴就全球法规事宜开展合作

05. 投资并探索多种注重隐私的解决方案
06. 扩充并激活您的第一方数据
07. 利用 Google 资源获得培训和其他指导



谢谢

Google