APP 隐私安全问题合规指引

问题一

违规收集个人信息

场景一

APP 在征求用户同意环节，未提供明确的同意或拒绝按钮，或者使用“好的”“我知道了”等词语。

场景二

APP 在征求用户同意环节，设置为默认勾选。

「场景一、二 」的合规建议

1. APP 在征询用户同意环节，应提供明确的同意和拒绝选项，不应仅使用“好的”、“我知道了”等无法清晰表达用户同意的词语；
2. APP 在征求用户同意时，应避免默认勾选同意等情形，将决定权交给用户。

场景三

APP 未见向用户明示个人信息收集使用的目的、方式和范围，未经用户同意，存在收集 XXX 的行为。

场景四

APP 未见向用户明示 SDK 收集使用个人信息的目的、方式和范围，未经用户同意，SDK 存在收集 XXX 的行为。

场景五

APP 以隐私政策弹窗的形式向用户明示收集使用规则，未经用户同意，存在收集 XXX 的行为。

场景六

APP 向用户明示 SDK 的收集使用规则，未经用户同意，SDK 存在收集 XXX 的行为。

「场景三、四、五、六 」的合规建议

APP 应以隐私弹窗等显著形式向用户清晰明示 APP 及集成 SDK 关于个人信息处理的目的、方式和范围，并需要在用户同意授权后，才可以收集用户个人信息或调用可收集个人信息的权限。

解决方案

1. 如果是自有代码的收集信息行为，需要调整代码后置收集信息行为；

2. 如果是集成 SDK 收集信息行为，需要把 SDK 初始化行为调整到玩家授权同意隐私协议政策后；
3. 如果自查依旧无法定位问题，可以咨询 TapTap 官方获取问题详情。

场景七

APP 以隐私政策弹窗的形式向用户明示收集使用规则，但未见清晰明示 APP 收集 XXX 等的目的方式范围，用户同意隐私政策后，存在收集 XXX 的行为。

场景八

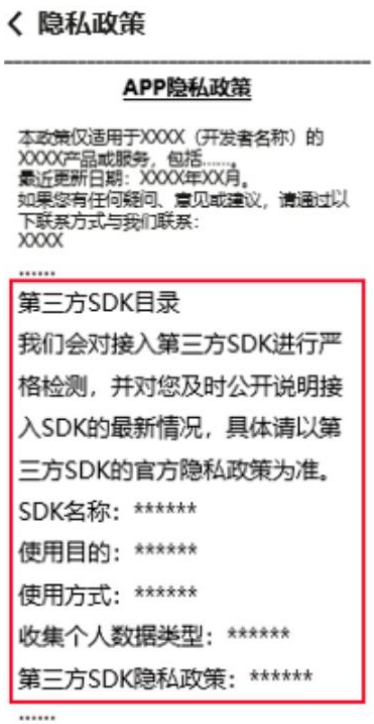
APP 向用户明示 SDK 的收集使用规则，但未见清晰明示 SDK 收集 XXX 等的目的方式范围，用户同意隐私政策后，SDK 存在收集 XXX 的行为。

「场景七、八 」的合规建议

隐私政策的弹窗中至少要包含《隐私政策》、《第三方信息共享清单》两部分内容。其中，《隐私政策》用于向用户说明 APP 自身收集使用用户信息的情况，《第三方信息共享清单》用于说明 APP 中第三方 SDK 收集使用个人信息的情况。

解决方案

1. 建议根据《个人信息安全检测报告》中描述的「个人信息行为 」完善 APP 或集成 SDK 收集信息的使用规则、目的、方式及范围；
2. 《第三方信息共享清单》的文本格式可参考下图。



经典案例

问题描述一

APP 内未设置隐私政策协议，玩家首次安装启动 APP 后可以直接进入游戏体验。

合规建议

依据国家相关政策要求，应该在用户授权同意隐私政策协议之后，再进行申请收集信息和获取权限的行为。因此建议在首次启动 APP 时以弹窗等显著的方式提示用户阅读并授权隐私政策协议，模板可参考上海市网络游戏行业协会提供的隐私政策示范文本进行编写。

问题描述二

Unity 3D SDK 在玩家授权同意隐私政策协议前获取信息的行为。

合规建议

将获取信息的行为调整为玩家授权后再初始化 SDK 。

1.确保游戏内设置了隐私政策协议，并以弹窗等显著形式展示协议，同时需要在隐私政策协议里清晰声明 unity 3D 相关内容；

第三方 SDK 名称：Unity 3D

应用场景： 框架

可能收集的个人信息的类型：读取设备信息（设备型号、系统名称、系统版本、MAC 地址、IMEI、Android ID）、访问相机、应用安装列表、任务列表、网络状态信息、设备传感器）

第三方 SDK 提供方：Unity Technologies

隐私政策链接：Privacy Policy

2.调整代码逻辑（以下任选其一）：

方案一

将 Unity 项目导出为 Android 工程，在 Android Studio 中为游戏新增一个上层 Activity 用于进行隐私政策展示与授权。

详情可参考：

https://taptap-privacy-compliance.oss-cn-shanghai.aliyuncs.com/report/Unity 导出安卓工程并新建 activity 用于放置隐私协议.pdf

方案二

1. 建议您更新 CN 版本的 Unity 到最新的 LTS 版本；

2. 检查 Unity Analystics 相关服务，先把 Analysitics 做一个延迟初始化（默认是启动 Unity 即初始化），待隐私同意后再进行初始化。然后查找是否用了 IAP 的包， IAP 包有缺陷，即只要工程里面含有这个包，启动必获取 Android ID，无法屏蔽，建议先移除这个包再重新打包。

问题描述三

APP 或集成 SDK 在玩家授权前同意隐私政策协议前获取传感器信息。

合规建议

建议调整获取传感器信息的行为到玩家同意隐私政策后进行。

问题描述四

未在游戏内的隐私政策协议披露传感器信息。

合规建议

建议在隐私政策协议里明示获取传感器信息的使用规则、目的、方式及范围。例如：

1. 当你播放视频等内容时，为了适配你的设备状态，我们会调用设备的重力、加速度等传感器，以识别你的设备横竖屏状态；
2. 你使用 XX 提供的道具、特效、滤镜、贴纸等工具拍摄并发布内容时，我们会根据你的操作及使用的工具类型使用加速度传感器、陀螺仪传感器、重力传感器等设备传感器，以适配你选用的工具。

问题二

超范围收集个人信息

场景一

APP 未见向用户告知且未经用户同意，在业务功能中，存在收集 XXX 等信息的行为，非服务所必需且无合理应用场景，超出与收集个人信息时所声称的目的具有直接或合理关联的范围。

「场景一 」的合规建议

APP 应以隐私弹窗等显著形式向用户清晰明示 APP 及集成 SDK 在各服务场景所需收集的通讯录、短信、通话记录、相机等 信息的行为、目的、规则及必要性，并在收集前征求用户同意。同时，所收集的个人信息不能超出其所明示收集目的的合理关联范围。

场景二

APP 在运行时，未见向用户告知且未经用户同意，存在每 30s 读取一次 XXX 信息，非服务所必需且无合理应用场景，超出实现产品或服务的业务功能所必需的最低频率。

场景三

APP 未见向用户明示 SDK 的收集使用规则，未经用户同意，SDK 存在每 30s 读取一次 XXX 信息，非服务所必需且无合理应用场景，超出实现产品或服务的业务功能所必需的最低频率。

场景四

APP 未见向用户告知且未经用户同意，在 YYY 功能中，存在收集通讯录、短信、通话记录、相机等信息的行为，非服务所必需且无合理应用场景，超出与收集个人信息时所声称的目的具有直接或合理关联的范围。

「场景二、三、四 」的合规建议

1. 建议在隐私政策中清晰明示各服务场景所需收集的地理位置信息的行为，并在收集前征求用户同意。如有频繁读取位置信息的场景，在隐私政策中明示说明频繁读取位置信息的必要性和频率；
2. APP 在提供对数据没有强实时性要求的功能服务时，建议尽量采用缓存的方式采集或上报设备信息，不要重新调用系统 API 数据。

场景五

APP 未见向用户告知且未经用户同意，在静默状态下或在后台运行时，存在收集通讯录、短信、通话记录、相机等信息的行为，非服务所必需且无合理应用场景，超出与收集个人信息时所声称的目的具有直接或合理关联的范围。

场景六

APP 未向用户明示 SDK 的收集使用规则，未经用户同意，SDK 在静默状态下或在后台运行时，存在收集通讯录、短信、通话记录、相机等信息的行为，非服务所必需且无合理应用场景，超出与收集个人信息时所声称的目的具有直接或合理关联的范围。

场景七

APP 未见向用户告知且未经用户同意，在静默状态下或在后台运行时，存在按照一定频次收集位置信息、IMEI、通讯录、短信、图片等信息的行为，非服务所必需且无合理应用场景，超出与收集个人信息时所声称的目的具有直接或合理关联的范围。

场景八

APP 未向用户明示 SDK 的收集使用规则，未经用户同意，SDK 在静默状态下或在后台运行时，存在按照一定频次收集位置信息、IMEI、通讯录、短信、图片等信息的行为，非服务所必需且无合理应用场景，超出与收集个人信息时所声称的目的具有直接或合理关联的范围。

「场景五、六、七、八 」的合规建议

1. APP 应在隐私政策中明示各服务场景所需收集的通讯录、短信、通话记录、相机等 信息的行为，且明示其必要性，并在收集前征求用户同意；
2. 如有静默状态或在后台运行 时存在收集通讯录、短信、通话记录、相机等信息的行为，在隐私政策中明示说明其必要性；
3. APP 在静默状态下或在后台运行时，APP 未向用户提供服务时，APP 本身及集成的 SDK 不应超出其所明示收集目的的合理关联范围，游戏后台获取个人信息的频率每分钟不超过 1 次。

问题三

违规使用个人信息

场景一

APP 未见向用户告知且未经用户同意，存在将 IMEI/ 设备 MAC 地址 / 软件安装列表等个人信息发送给友盟 / 极光 / 个推等第三方 SDK 的行为。

「场景一 」的合规建议

APP 应以《第三方服务共享清单》等显著形式清晰描述接入的主要的第三方服务商、涉及的数据类型、使用目的、处理方式等内容，并需要在用户同意授权后，才可以向第三方服务商发送用户的个人信息内容。

场景二

APP 未见向用户明示分享的第三方名称、目的及个人信息类型，用户同意隐私政策后，存在将 IMEI / 设备 MAC 地址 / 软件安装列表等个人信息发送给友盟/极光/个推等第三方 SDK 的行为。

「场景二 」的合规建议

APP 以隐私政策协议弹窗等显著形式向用户明示个人信息处理目的、方式和范围，应逐一列明，不应使用“等”这样的模糊描述。

问题四

强制用户使用定向推送功能

场景一

APP 的 YYY 页面或功能存在定向推送功能，但隐私政策未见向用户告知，将收集的用户个人信息用于定向推送、精准营销。

场景二

APP 隐私政策存在“根据您的偏好进行个性化推荐 YYYY ”等内容，明示存在定向推送功能，但页面中未见显著区分个性化推送服务，如标明“个性化展示”或“定推”等字样。

可能性一

游戏内提供了个性化或定向推送的功能服务，将收集到的用户搜索、浏览记录、使用习惯等个人信息，用于定向推送或广告精准营销。

「场景一、二 」的合规建议

1. 隐私政策协议里清晰说明服务内容，用途等；
2. 游戏标明服务的内容，增加「 个性化、猜你喜欢」等描述；
3. 在游戏内的设置位置设置显著关闭相关服务的按钮。

可能性二

游戏内提供了个性化或定向推送的功能服务。

解决方案

隐私协议里的内容需要和游戏内实际提供的服务一致，隐私政策协议中请不要说明相关服务内容，或者明确说明不提供定向推送功能。

问题五

APP 强制、频繁、过度索取权限

场景一

APP 首次启动时，向用户索取电话、通讯录、定位、短信、录音、相机、存储、日历等权限，用户拒绝授权后，应用退出或关闭（应用陷入弹窗循环，无法正常使用）。

「 场景一」的合规建议

用户拒绝授权后，App 仍需要向用户提供基础功能。

场景二

APP 首次打开（或其他时机），未见使用权限对应的相关产品或服务时，提前向用户弹窗申请开启通讯录 / 定位 / 短信 / 录音 / 相机 /XXX 等权限。

场景三

APP 运行时，未向用户告知 XXX 权限的目的，向用户索取当前服务场景未使用到的通讯录、定位、短信、录音、相机、日历等权限，且用户拒绝授权后，应用退出或关闭相关功能，无法正常使用。

场景四

用户注册登录时，APP 向用户索取电话 / 通讯录 / 定位 / 短信 / 录音 / 相机 / 存储 / 日历等权限，用户拒绝授权后，应用无法正常注册或登录。

场景五

APP 运行时，向用户索取当前服务场景未使用到的电话 / 通讯录 / 定位 / 短信 / 录音 / 相机 / 存储 / 日历等权限，且用户拒绝授权后，应用退出或关闭（应用陷入弹窗循环，无法正常使用）。

场景六

APP 运行时，在用户明确拒绝通讯录 / 定位 / 短信 / 录音 / 相机 /XXX 等权限申请后，仍向用户频繁弹窗申请开启与当前服务场景无关的权限，影响用户正常使用。

「场景二、三、四、五、六 」的合规建议

1. 隐私政策协议里需要明示功能服务的使用场景及需要获取的权限；
2. 关于 Android 应用的权限申请与使用，可以参照《网络安全标准实践指南—移动互联网应用程序（App）系统权限申请使用指南》(全国信息安全标准化技术委员会)进行描述；
3. APP 首次打开或运行中，未见使用权限对应的相关功能或服务时，不应提前向用户申请权限。用户拒绝授权后，APP 不应退出、关闭相关功能服务、频繁弹窗等限制影响用户正常使用；
4. 对于用户无法明确感知到权限使用场景的情况下应采用单独弹窗的形式向用户说明权限申请目的。

场景七

APP 在用户明确拒绝通讯录 / 定位 / 短信 / 录音 / 相机 /XXX 等权限申请后，重新运行时，仍向用户弹窗申请开启与当前服务场景无关的权限，影响用户正常使用。

「 场景七」的合规建议

用户拒绝授权后，APP 不应退出、关闭相关功能服务、频繁弹窗等限制影响用户正常使用。并且建议在 48 小时内不得重复申请权限。

问题六

APP 频繁自启动和关联启动

场景一

APP 未向用户明示未经用户同意，且无合理的使用场景，存在频繁自启动或关联启动的行为。

场景二

APP 非服务所必需或无合理应用场景，超范围频繁自启动或关联启动第三方 APP。

「场景一、二」的合规建议

1. 如业务必需要自启动或关联启动第三方 APP，请在隐私政策中说明相关场景及频次；
2. 如此场景业务无合理理由，建议移除自启动的服务。

一般情况下，导致自启进程的可能有如下几种情况：

可能性一

manifest 配置文件中注册的系统广播监听导致的自启动行为（例如监听开机动作、监听网络变化等）。解决方案：

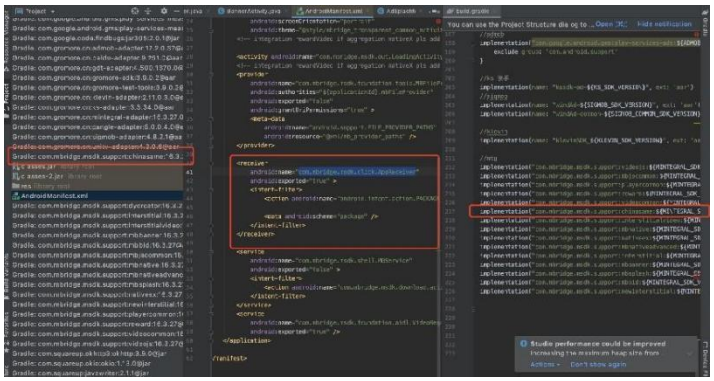
1. 移除 manifest 中注册的非必要系统广播监听；
2. 尽可能设置所有 service onStartCommand（方法返回 START_NOT_STICKY）；
3. 如果自查依旧无法定位问题，可以咨询 TapTap 官方获取问题详情。

可能性二

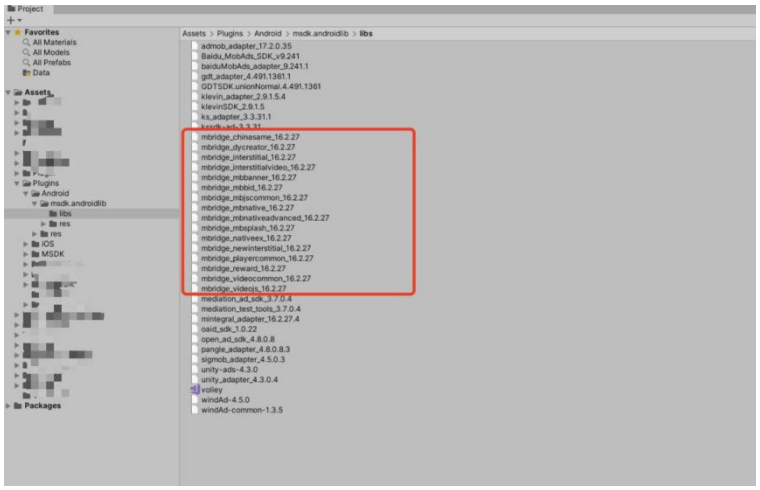
com.mbridge.msdk 导致的自启行为，可以先尝试如下方法解决：

1、先确定自己接入的 Gromore SDK 版本是否为最新版，如果不是，先更新版本；

2、如果接入的是 Gromore SDK_Android，自启动风险是穿山甲 SDK 集成的第三方网络 mtg 的问题，如果没有接入 mtg 网络可以尝试将依赖去掉解决；



3、如果你接入的是 Gromore SDK_unity，可以尝试在 unity 工程文件中参考下图移除相关 libs 解决。



可能性三

TapSDK 导致的关联自启行为，建议您更新升级 TapSDK 至 3.16.4 版本以上。

场景三

APP 虽然有向用户明示并经用户同意环节，但频繁自启动或关联启动发生在用户同意前。

「 场景三」的合规建议

建议调整自启动或关联启动行为到用户授权同意隐私政策协议之后再进行。