艾思科蓝-会议期刊论文发表

隐私与合规检测报告

2024年12月24日

任务/应用名称	艾思科蓝-会议期刊论文发表
检测版本号	2.2.1
任务包名	com.keo.ais.main
SHA256	ac6a2c7db5949283adf13210c69a7ebd57f849b968717c29deb7f0f282e776e6
检测结果	存在问题

使用须知

1. 为了得到更准确全面的检测结果，请上传未加固的包进行检测。

2. 由于检测内容和方法的局限，本报告中的部分评估项检测结果可能存在偏差，必要时请进行人工核验结果。

3. 本报告为技术性检测报告，不属于法律分析意见，仅用于帮助您发现被检测APP的隐私合规风险。

4. 请勿将本报告用于侵犯任何第三方名誉或商誉、隐私、知识产权和其他合法权益的活动。

5.禁止将报告用于其他商业目的，本报告仅限vivo开放平台开发者阅读。

1. 隐私与合规检测依据

序号	法律法规
01	《T/TAF 078.1-2020 App用户权益保护测评规范》
02	《App违法违规收集使用个人信息行为认定方法》
03	《工业和信息化部关于开展纵深推进APP侵害用户权益专项整治行动的通知（工信部信管函【2020】164号）》
04	《工业和信息化部关于进一步提升移动互联网应用服务能力的通知（工信部信管函【2023】26号）》

2. 检测结果： 存在问题

2.1 工信部信管函［2020］164号文/工信部信管函［2023］26号检测结果概览

序号	检测类型	结果
01	超范围收集个人信息	发现问题
02	违规收集个人信息	未发现问题及风险
03	违规使用个人信息	未发现问题及风险
04	APP强制、频繁、过度索取权限	未发现问题及风险
05	APP频繁自启动和关联启动	未发现问题及风险
06	强制用户使用定向推送功能	未发现问题及风险
07	欺骗误导用户提供个人信息	暂不支持自动化检测，请进行人工自评
08	欺骗误导强迫行为	未发现问题及风险
09	应用分发平台责任落实不到位	暂不支持自动化检测，请进行人工自评

2.2 工信部信管函［2020］164号文/工信部信管函［2023］26号检测结果 （共57 项）

序号	类型	数量
01	发现问题	1
02	未发现问题及风险	38
03	暂不支持自动化检测，请进行人工自评	18

3. 工信部信管函［2020］164号文/工信部信管函［2023］26号检测结果详情

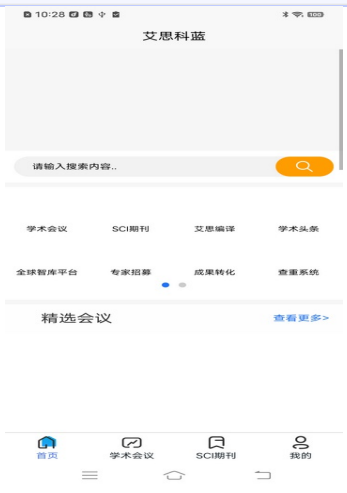
3.1 隐私测试未通过详情

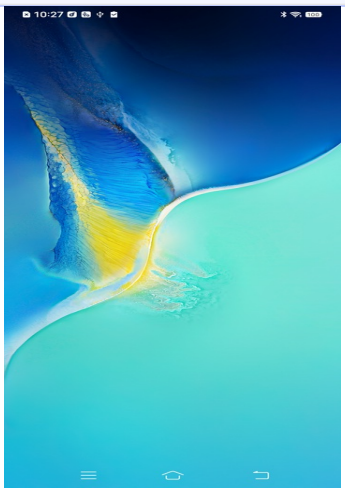
发现问题	问题类型：SDK点击一次收集一次或以上个人信息

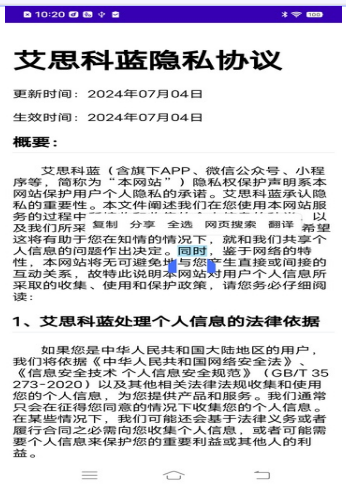
APP在运行时，第三方SDK存在以下违规行为：

1、未见使用场景，Weex存在点击一次至少采集一次"剪切板信息"的行为，非服务所必须且无合理应用场景，超出实现产品或服务的业务功能所必须的最低频率

对应条款： APP在运行时，未见向用户告知且未经用户同意，在点击功能时，SDK存在每点击一次至少收集一次 IMEI、IMSI、设备 MAC 地址、Android ID、OAID、MEID、ICCID、SN、SUCI、SUPI、软件安装列表、位置、联系人、通话记录、日历、短信、本机电话号码、图片、音视频等个人信息的行为，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







举证信息

2024-12-24

10:30:17 Weex读取剪贴板内容

合规建议 1、确保第三方SDK收集个人信息的频率不超出其实现产品或服务的业务功能所必需的最低频率

2、若需要以特定频次收集用户个人信息，需要确保必要性，同时在隐私政策中告知用户APP收集相关个人信息的频率

3.2 隐私测试报告详情

3.2.1 超范围收集个人信息

超范围收集:

1. APP收集 IMEI、IMSI、设备 MAC 地址、Android ID、OAID、MEID、ICCID、SN、SUCI、SUPI、软件安装列表、位置、联系人、通话记录、日历、短信、本机电话号码、图片、音视频等个人信息的行为时，超出其所明示收集目的的直接关联范围
2. APP仅以服务体验、产品研发、算法推荐、风险控制等为由，强制要求用户同意超范围或者与服务场景无关的个人信息处理行为

检测结果 **暂不支持自动化检测，请进行人工自评**

合规建议 1、APP不应超出其业务服务范围收集个人信息

2、APP不应该仅以服务体验、产品研发、算法推荐、风险控制等为由，强制要求用户同意超范围或者与服务场景无关的个人信息处理行为

自查方式 1、梳理APP所有需要使用个人信息的服务和功能，以及其对应的的个人信息字段

2、参考《常见类型移动互联网应用程序必要个人信息范围规定》确定APP基本业务的必要信息范围，确认基本服务是否存在超范围收集用户个人信息

3、判断APP附加服务采集的信息类型是否超出其业务功能的必要信息范围，即缺少该字段是否可以继续为用户提供服务。

4、若存在第二步或第三步所提及的情况，可判断此项存在问题

超频次收集:

APP存在收集 IMEI、IMSI、设备 MAC 地址、Android ID、OAID、MEID、ICCID、SN、SUCI、SUPI、软件安装列表、位置、联系人、通话记录、日历、短信、本机电话号码、图片、音视频等个人信息的行为，超出实现产品或服务的业务功能所必需的最低频率

检测结果 **未发现问题**

SDK超范围收集:

SDK收集 IMEI、IMSI、设备 MAC 地址、Android ID、OAID、MEID、ICCID、SN、SUCI、SUPI、软件安装列表、位置、联系人、通话记录、日历、短信、本机电话号码、图片、音视频等个人信息的行为，超出其所明示收集目的的直接关联范围

检测结果 暂不支持自动化检测，请进行人工自评

合规建议 APP向用户明示第三方SDK处理个人信息的目的、方式和范围。SDK不应超出其业务服务范围收集收集上述个人信息

自查方式 1、判断SDK所相关服务采集的信息类型是否超出其业务功能的必要信息范围，即缺少该字段是否可以继续为用户提供服务。

2、若存在第一步所提及的情况，可判断此项存在问题

SDK超频次收集:

SDK存在收集IMEI、IMSI、设备 MAC 地址、Android ID、OAID、MEID、ICCID、SN、SUCI、SUPI、软件安装列表、位置、联系人、通话记录、日历、短信、本机电话号码、图片、音视频等个人信息的行为，超出实现产品或服务的业务功能所必需的最低频率

检测结果 未发现问题

静默后台超范围收集:

APP在静默状态下或在后台运行时，收集IMEI、IMSI、设备 MAC 地址、Android ID、OAID、MEID、ICCID、SN、SUCI、SUPI、软件安装列表、位置、联系人、通话记录、日历、短信、本机电话号码、图片、音视频等个人信息，超出其所明示的收集目的的合理关联范围

检测结果 未发现问题

静默后台超频次收集:

APP在静默状态下或在后台运行时，收集IMEI、IMSI、设备 MAC 地址、Android ID、OAID、MEID、ICCID、SN、SUCI、SUPI、软件安装列表、位置、联系人、通话记录、日历、短信、本机电话号码、图片、音视频等个人信息，超出实现产品或服务的业务功能所必需的最低频率

检测结果 未发现问题

SDK静默后台超范围收集:

SDK在静默状态下或在后台运行时，收集 IMEI、IMSI、设备 MAC 地址、Android ID、OAID、MEID、ICCID、SN、SUCI、SUPI、软件安装列表、位置、联系人、通话记录、日历、短信、本机电话号码、图片、音视频等个人信息，超出其所明示的收集目的的合理关联范围

检测结果 未发现问题

SDK静默后台超频次收集:

SDK在静默状态下或在后台运行时，收集 IMEI、IMSI、设备 MAC 地址、Android ID、OAID、MEID、ICCID、SN、SUCI、SUPI、软件安装列表、位置、联系人、通话记录、日历、短信、本机电话号码、图片、音视频等个人信息，超出实现产品或服务的业务功能所必需的最低频率

检测结果 未发现问题

SDK初始化超范围收集个人信息:

APP首次运行，用户同意隐私政策后，非服务所必须且无合理应用场景，SDK存在收集 IMEI、IMSI、设备 MAC 地址、Android ID、OAID、MEID、ICCID、SN、SUCI、SUPI、软件安装列表、位置、联系人、通话记录、日历、短信、本机电话号码、图片、音视频等个人信息的行为，超出其所明示的收集目的的合理关联范围

检测结果 未发现问题

点击一次收集一次或以上个人信息:

APP在运行时，未见向用户告知且未经用户同意，在点击功能时，存在每点击一次至少收集一次 IMEI、IMSI、设备 MAC 地址、Android ID、OAID、MEID、ICCID、SN、SUCI、SUPI、软件安装列表、位置、联系人、通话记录、日历、短信、本机电话号码、图片、音视频等个人信息的行为，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

检测结果 未发现问题

SDK点击一次收集一次或以上个人信息:

APP在运行时，未见向用户告知且未经用户同意，在点击功能时，SDK存在每点击一次至少收集一次 IMEI、IMSI、设备 MAC 地址、Android ID、OAID、MEID、ICCID、SN、SUCI、SUPI、软件安装列表、位置、联系人、通话记录、日历、短信、本机电话号码、图片、音视频等个人信息的行为，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

检测结果

发现问题

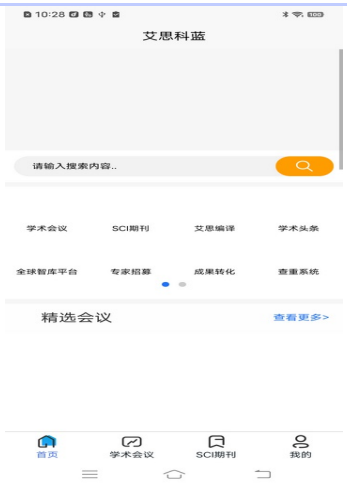
APP在运行时，第三方SDK存在以下违规行为：

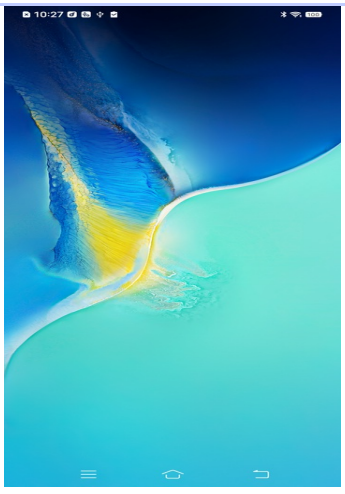
1、未见使用场景，Weex存在点击一次至少采集一次"剪切板信息"的行为，非服务所必须且无合理应用场景，超出实现产品或服务的业务功能所必须的最低频率

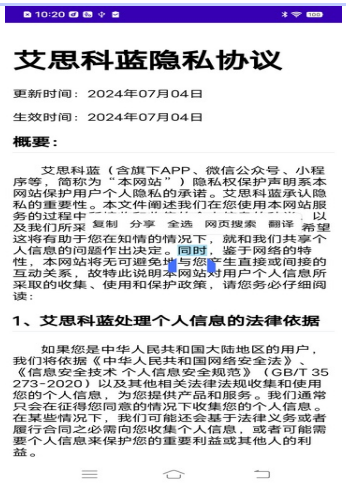
合规建议 1、确保第三方SDK收集个人信息的频率不超出其实现产品或服务的业务功能所必需的最低频率

2、若需要以特定频次收集用户个人信息，需要确保必要性，同时在隐私政策中告知用户APP收集相关个人信息的频率

举证信息







2024-12-24

10:30:17 Weex读取剪贴板内容

固定频次收集个人信息:

APP在运行时，未见向用户告知且未经用户同意，以固定频率收集 IMEI、IMSI、设备 MAC 地址、Android ID、OAID、MEID、ICCID、SN、SUCI、SUPI、软件安装列表、位置、联系人、通话记录、日历、短信、本机电话号码、图片、音视频等个人信息的行为，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

检测结果 **未发现问题**

SDK固定频次收集个人信息:

APP在运行时，未见向用户告知且未经用户同意，SDK以固定频率收集 IMEI、IMSI、设备 MAC 地址、Android ID、OAID、MEID、ICCID、SN、SUCI、SUPI、软件安装列表、位置、联系人、通话记录、日历、短信、本机电话号码、图片、音视频等个人信息的行为，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

检测结果 **未发现问题**

3.2.2 违规收集个人信息

未见明示收集:

APP 未以弹窗等形式向用户明示个人信息处理的目的、方式和范围，收集收集IMEI、IMSI、设备 MAC 地址、Android ID、OAID、MEID、ICCID、SN、SUPI、SUCI、软件安装列表、位置、联系人、通话记录、日历、短信、本机电话号码、图片、音视频、剪切板等个人信息

检测结果 **未发现问题**

有明示未同意收集:

APP 以弹窗等形式向用户明示个人信息处理的目的、方式和范围，未经用户同意，收集 IMEI、IMSI、设备 MAC 地址、Android ID、OAID、MEID、ICCID、SN、SUPI、SUCI、软件安装列表、位置、联系人、通话记录、日历、短信、本机电话号码、图片、音视频、剪切板等个人信息

检测结果 **未发现问题**

明示不清晰收集:

APP 以弹窗等形式向用户明示个人信息处理的目的、方式和范围，未清晰明示处理 IMEI、IMSI、设备 MAC 地址、Android ID、OAID、MEID、ICCID、SN、SUPI、SUCI、软件安装列表、位置、联系人、通话记录、日历、短信、本机电话号码、图片、音视频、剪切板等个人信息的目的、方式和范围，用户同意后，收集相应个人信息

检测结果 未发现问题

未见明示SDK收集:

APP 未以弹窗等形式向用户明示第三方 SDK 处理个人信息的目的、方式和范围，第三方 SDK 收集 IMEI、IMSI、设备 MAC 地址、软件安装列表等个人信息

检测结果 未发现问题

明示SDK未同意收集:

APP 以弹窗等形式向用户明示第三方 SDK 处理个人信息的目的、方式和范围，未经用户同意，第三方 SDK 收集 IMEI、IMSI、设备 MAC 地址、Android ID、OAID、MEID、ICCID、SN、SUPI、SUCI、软件安装列表、位置、联系人、通话记录、日历、短信、本机电话号码、图片、音视频、剪切板等个人信息

检测结果 未发现问题

明示SDK不清晰收集:

APP 以弹窗等形式向用户明示第三方 SDK 处理个人信息的目的、方式和范围，未清晰明示第三方 SDK 处理 IMEI、IMSI、设备 MAC 地址、Android ID、OAID、MEID、ICCID、SN、SUPI、SUCI、软件安装列表、位置、联系人、通话记录、日历、短信、本机电话号码、图片、音视频、剪切板等个人信息的目的、方式和范围，用户同意后，第三方 SDK 收集相应个人信息

检测结果 未发现问题

同意不清晰:

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

检测结果 未发现问题

默认同意:

APP 在征求用户同意环节，设置为默认同意

检测结果 未发现问题

未突出展示敏感个人信息:

APP个人信息处理规则中未突出展示APP处理个人敏感信息的目的、方式和范围

检测结果 **暂不支持自动化检测，请进行人工自评**

合规建议 APP隐私政策协议中，需要用加粗、下划线等方式突出展示个人敏感信息及其处理的目的、方式和范围

自查方式 1、梳理APP个人信息处理情况，查看是否涉及到个人敏感信息

2、查看隐私政策协议中，是否使用加粗、下划线等方式，突出展示个人敏感信息及其处理的目的、方式、范围

SDK未突出展示敏感个人信息:

APP个人信息处理规则中未突出展示SDK处理个人敏感信息的目的、方式和范围

检测结果 **暂不支持自动化检测，请进行人工自评**

合规建议 APP隐私政策协议中，需要用加粗、下划线等方式突出展示SDK个人敏感信息及其处理的目的、方式和范围

自查方式 1、梳理SDK个人信息处理情况，查看是否涉及到个人敏感信息

2、查看隐私政策协议中，是否使用加粗、下划线等方式，突出展示个人敏感信息及其处理的目的、方式、范围

拒绝同意:

用户拒绝提供非当前服务所必需的个人信息时，APP拒绝用户使用该服务的基本功能。

检测结果 **暂不支持自动化检测，请进行人工自评**

合规建议 用户拒绝提供非当前服务所必须的个人信息时，APP需要向用户提供该服务基本功能

自查方式 1、梳理APP所有需要使用个人信息的服务和功能，以及其对应的的个人信息字段

2、参考《常见类型移动互联网应用程序必要个人信息范围规定》确定APP基本业务的必要信息范围，确认基本服务是否存在超范围收集用户个人信息

3、判断APP附加服务采集的信息类型是否超出其业务功能的必要信息范围，即缺少该字段是否可以继续为用户提供服务。

4、若存在第二步或第三步所提及的情况，可判断此项存在问题

3.2.3 违规使用个人信息

未明示或同意共享:

APP 未向用户明示个人信息处理的目的、方式和范围，或未经用户同意，将 IMEI、IMSI、设备 MAC 地址、SUPI、SUCI、软件安装列表、位置、联系人、通话记录、日历、短信、本机电话号码、图片、音视频等个人信息发送给第三方 SDK 等产品或服务

检测结果 未发现问题

明示共享不清晰:

APP 以弹窗等形式向用户明示个人信息处理的目的、方式和范围，未清晰明示共享的第三方身份、目的及个人信息类型，用户同意后，将IMEI、IMSI、设备 MAC 地址、SUPI、SUCI、软件安装列表、位置、联系人、通话记录、日历、短信、本机电话号码、图片、音视频等个人信息发送给第三方 SDK 等产品或服务

检测结果 未发现问题

服务器端共享:

APP 未向用户告知且未经用户同意，将设备识别信息、商品浏览记录、搜索使用习惯、软件安装列表等个人信息传输至 APP 服务器后，向第三方产品或服务提供其收集的个人信息

检测结果 **暂不支持自动化检测，请进行人工自评**

合规建议 APP中涉及到个性化推荐的服务，需要通过隐私政策弹窗等方式向用户进行明示，并获取同意

自查方式 1、确认个人数据被传输到服务器后是否存在与第三方共享的行为

2、若存在，确认相关共享行为是否在隐私政策中进行说明，并获取用户同意

3、若未进行说明且未获取用户同意，则判断此项存在问题

3.2.4 欺骗误导强迫行为

信息窗口关不掉:

APP在用户终端弹出广告或者其他与终端软件功能无关的信息窗口的，未以显著的方式向用户提供关闭或者退出窗口的功能标识，或提供虚假、无效、标识不明显的关闭选项。

检测结果 未发现问题

点击任意位置下载:

APP信息窗口页面，下载、安装、使用第三方APP时，未以显著方式明示，或未经用户主动选择同意，点击任意位置即自动下载、安装、使用第三方APP

检测结果 未发现问题

误导下载:

APP信息窗口页面，通过虚假、引人误解的方式欺骗误导强迫用户下载、安装、使用第三方APP的行为，包括但不限于在未明示下载APP的情况下，通过“是否立即开始游戏”、“领取红包”、“手机卡顿”、“耗电太快”、“内存已满”等方式

检测结果 未发现问题

未提供暂停选项:

APP分发页面在用户点击下载后未同步展示下载进度并提供暂停、取消选项，或未以显著方式告知在任务栏、链接至下载中心等位置展示下载进度及提供暂停、取消选项

检测结果 **暂不支持自动化检测，请进行人工自评**

合规建议 APP分发页面需要确保：

1、用户点击下载后同步展示下载进度，同时提供暂停、取消选项，或；

2、其他显著方式告知用户展示下载进度，同时提供暂停、取消选项

自查方式 1、确认APP是否存在分发页面

2、点击任意APP进行下载，查看是否同步展示下载进度，同时提供暂停、取消选项或以显著方式告知在任务栏、链接至下载中心等位置展示下载进度及提供暂停、取消选项

强迫更新:

非服务所必需或无合理场景，以弹窗等方式强迫用户进行更新

检测结果 未发现问题

强迫下载:

以折叠显示、主动弹窗、频繁提示等方式强迫用户下载、打开APP

检测结果 **暂不支持自动化检测，请进行人工自评**

合规建议 APP不应以折叠显示、主动弹窗、频繁提示等方式强迫用户下载、打开第三方APP

自查方式 APP运行中查看是否存在以折叠显示、主动弹窗、频繁提示等方式强迫用户下载、打开APP

自动下载:

APP信息窗口页面在用户无操作情况下自动下载、安装、使用第三方APP

检测结果 未发现问题

自动恢复下载:

用户暂停或取消下载、安装的APP自动恢复下载安装

检测结果 **暂不支持自动化检测，请进行人工自评**

合规建议 用户暂停或取消下载、安装的APP不应自动恢复下载安装

自查方式 1、暂停或取消下载、安装第三方APP，

2、关闭并重新运行本APP后，查看被暂停或取消下载的第三方APP是否自动恢复下载。

宣传不符:

APP信息窗口页面，下载、安装、使用的APP与向用户所作的宣传或者承诺不符

检测结果 **暂不支持自动化检测，请进行人工自评**

合规建议 APP信息窗口页面，下载、安装、使用的APP与向用户所作的宣传或者承诺一致

自查方式 1、针对APP信息窗口页面，若存在下载、安装、使用APP的功能，按照相关描述进行功能触发

2、查看下载、安装、使用的APP是否与向用户所作的宣传或者承诺不符

应用难卸载:

APP以空白名称、透明图标、后台隐藏等方式欺骗用户，阻挠用户进行真实有效的卸载操作

检测结果 **暂不支持自动化检测，请进行人工自评**

合规建议 APP不应以空白名称、透明图标、后台隐藏等方式欺骗用户，阻挠用户进行真实有效的卸载操作

自查方式 卸载APP，查看是否存在以空白名称、透明图标、后台隐藏等方式欺骗用户，阻挠用户进行真实有效的卸载操作

欺骗误导点击跳转:

a） APP以欺骗、误导或者强迫等方式向用户提供互联网信息服务或者产品；

b） 未以显著方式明示或未经用户主动选择同意，APP信息窗口页面，存在跳转、使用第三方的行为；

c） APP信息窗口页面，跳转、使用第三方时，存在欺骗误导强迫用户跳转的文字、图片或视频链接；

d） APP频繁弹窗干扰用户正常使用

检测结果 **暂不支持自动化检测，请进行人工自评**

合规建议 APP不应存在欺骗、误导用户点击跳转第三方APP的行为

自查方式 a） 确认APP是否存在以欺骗、误导或者强迫等方式向用户提供互联网信息服务或者产品；

b） 确认是否存在未以显著方式明示或未经用户主动选择同意，APP信息窗口页面，存在跳转、使用第三方的行为；

c） APP信息窗口页面，跳转、使用第三方时，确认APP是否存在欺骗误导强迫用户跳转的文字、图片或视频链接；

d） 确认APP是否存在频繁弹窗干扰用户正常使用的行为

摇一摇跳转:

APP信息窗口通过用户“摇一摇”等交互动作触发页面或第三方应用跳转的，未清晰明示用户需要执行的触发动作及交互预期，或通过设置高灵敏度降低交互动作判定阈值，造成误导、强迫式跳转

检测结果 未发现问题

3.2.5 应用分发平台责任落实不到位

应用分发平台上的 APP 信息明示不到位:

应用分发平台存在下述问题：

a) 应用分发平台下载页面所明示的 APP 的名称与下载安装后的 APP 名称不一致；

b) 应用分发平台未明示所分发 APP 的真实完整有效的开发者或运营者信息；

c) 应用分发平台明示的 APP 开发者或运营者信息与 APP 的隐私政策或用户协议等自声明中的开发者或运营者信息不一致

d) 应用分发平台未明示所分发 APP 的版本信息；

e) 应用分发平台下载页面未明示所分发 APP 的安装及运行所需权限列表及用途。

f) 应用分发平台下载页面未明示所分发 APP 的收集使用个人信息的内容、目的、方式和范围

检测结果 **暂不支持自动化检测，请进行人工自评**

合规建议 1、应用分发平台下载页面所明示的 APP 的名称与下载安装后的 APP 名称应一致；

2、应用分发平台应明示所分发 APP 的真实完整有效的开发者或运营者信息；

c) 应用分发平台明示的 APP 开发者或运营者信息与 APP 的隐私政策或用户协议等自声明中的开发者或运营者信息应一致

d) 应用分发平台应明示所分发 APP 的版本信息；

e) 应用分发平台下载页面应明示所分发 APP 的安装及运行所需权限列表及用途。

f) 应用分发平台下载页面应明示所分发 APP 的收集使用个人信息的内容、目的、方式和范围

自查方式 1、应用分发平台下载页面所明示的 APP 的名称与下载安装后的 APP 名称是否一致；

2、应用分发平台是否明示所分发 APP 的真实完整有效的开发者或运营者信息；

c) 应用分发平台明示的 APP 开发者或运营者信息与 APP 的隐私政策或用户协议等自声明中的开发者或运营者信息是否一致

d) 应用分发平台是否明示所分发 APP 的版本信息；

e) 应用分发平台下载页面是否明示所分发 APP 的安装及运行所需权限列表及用途。

f) 应用分发平台下载页面是否明示所分发 APP 的收集使用个人信息的内容、目的、方式和范围

应用分发平台责任落实不到位:

应用分发平台存在下述问题：

a) 应用分发平台在所分发的 APP 分发前，未对其严格审核；

b) 未确保所分发 APP 的软件提供者、运营者、开发者身份及其联系方式真实有效；

c) 应用分发平台未及时处理违规违规软件

检测结果 暂不支持自动化检测，请进行人工自评

合规建议 1、应用分发平台应确认在所分发的 APP 分发前，对其严格审核；

2、应用分发平台应确保所分发 APP 的软件提供者、运营者、开发者身份及其联系方式真实有效；

c) 应用分发平台应及时处理违规违规软件

自查方式 1、是否在所分发的 APP 分发前，对其严格审核；

2、APP 的软件提供者、运营者、开发者身份及其联系方式是否真实有效；

c) 是否及时处理违规违规软件

3.2.6 APP强制、频繁、过度索取权限

不给权限APP退出或关闭:

APP 运行时，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，APP 退出或关闭（循环弹窗）

检测结果 未发现问题

未告知申请权限目的:

APP运行时，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，未及时明确告知用户索取权限的目的和用途

检测结果 未发现问题

不给权限APP无法登录或注册:

APP 运行时，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，APP拒绝注册或登录

检测结果 未发现问题

申请无关权限:

APP 未提供相关业务功能或服务，申请对应权限

检测结果 未发现问题

拒绝权限后再次弹窗:

APP 运行时，在用户明确拒绝通讯录、定位、短信、录音、相机、日历、电话、存储、通知等权限申请后，向用户频繁弹窗申请与当前服务场景无关的权限，影响用户正常使用

检测结果 未发现问题

拒绝权限后重新启动再次弹窗:

APP 在用户明确拒绝通讯录、定位、短信、录音、相机、日历、电话、存储、通知等权限申请后，重新运行时，APP 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

检测结果 未发现问题

过度申请权限:

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，提前向用户弹窗申请开启通讯录、定位、短信、录音、相机、日历、电话、存储等权限

检测结果 未发现问题

过度申请功能非必须权限:

APP 运行时，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，APP 拒绝提供与申请权限无关的功能服务

检测结果 暂不支持自动化检测，请进行人工自评

合规建议 APP 运行时，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，APP不应拒绝提供与申请权限非强相关的功能服务

自查方式 1、梳理APP所有需要使用权限的服务和功能，以及其对应的权限

2、确认权限的申请是否超出其业务功能的必要范围，即缺少该权限是否可以继续为用户提供服务。例如：针对天气类、外卖类功能，地理位置为合理权限，可以方便用户使用相关服务，但是用户拒绝不应直接决绝相关功能的使用，可以提供手动搜索的功能。

3、若超出必要范围，用户拒绝后是否可以继续使用相关服务

4、若不能使用，则判断此项存在违规

3.2.7 欺骗误导用户提供个人信息

欺骗误导用户提供个人信息:

非服务所必需或无合理场景，APP 广告页面或功能页面，通过积分、奖励、优惠等方式欺骗误导用户提供身份证号码、人脸、指纹等个人信息的行为，则判定为欺骗诱导用户提供个人信息

检测结果 暂不支持自动化检测，请进行人工自评

合规建议 非服务所必需或无合理场景，APP 广告页面或功能页面，通过积分、奖励、优惠等方式欺骗误导用户提供身份证号码、人脸、指纹等个人信息

自查方式 1、确认APP是否采集身份证号码、人脸、指纹等个人信息

2、参考《常见类型移动互联网应用程序必要个人信息范围规定》确定APP基本业务是否需要采集身份证号码、人脸、指纹等个人信息，若不需要，但APP依然将上述信息作为开启应用的前提条件，则存在问题

3、若APP附加服务需要将身份证、人脸、指纹等个人信息作为功能使用的前提条件，判断是否超出其业务功能的必要信息范围，即缺少该字段是否可以继续为用户提供服务。

3、判断是否通过积分、奖励、优惠等方式诱导用户提供个人信息

4、若存在上述第一步、第二步或第三步所提及的情况，可判断此项存在问题

3.2.8 APP频繁自启动和关联启动

未见明示自启动:

APP 未向用户明示未经用户同意，且无合理的使用场景自启动或关联启动其它 APP

检测结果 未发现问题

有明示未同意自启动:

APP 向用户明示但未经用户同意，自启动或关联启动其它 APP

检测结果 未发现问题

无合理应用场景自启动或关联启动:

APP 或SDK非服务所必需或无合理应用场景，自启动或关联启动APP

检测结果 未发现问题

3.2.9 强制用户使用定向推送功能

未明示定推:

APP 的业务功能存在定向推送功能，未以个人信息处理规则弹窗等形式向用户明示，将收集的用户个人信息用于定向推送、精准营销

检测结果 未发现问题

未明示定推第三方个人信息来源:

APP 定向推送功能使用了第三方的个人信息，在进行定向推送时，未以个人信息处理规则弹窗等形式向用户明示业务功能使用了第三方的个人信息，或未向用户明示第三方的个人信息来源。

检测结果 暂不支持自动化检测，请进行人工自评

合规建议 APP定向推送功能若使用了第三方来源的个人信息，需要通过隐私政策弹窗等形式告知用户使用第三方来源的个人信息进行定向推送，同时向用户明示第三方个人信息来源，并获取其同意

自查方式 1、确认APP定向功能是否会使用到从第三方来源获取到的个人信息

2、若存在，确认APP隐私政策中是否说明第三方个人信息来源，并获取用户同意

3、若未进行说明且未获取用户同意，则判断此项存在问题

未标识定推:

APP 以个人信息处理规则弹窗等形式明示存在定向推送功能，页面中未显著区分定向推送服务。显著标识的方式包括但不限于：标明“个性化推荐”、“定推”、“猜你喜欢”等其他能显著区分的字样，或通过不同的栏目、版块、页面分别展示等

检测结果 暂不支持自动化检测，请进行人工自评

合规建议 APP中涉及到个性化推荐的服务，需要在功能使用过程中对用户进行明示，包括但不限于“个性化推荐”、“定向推送”、“猜你喜欢”等。

自查方式 1、查看APP隐私政策中是否存在个性化推荐相关内容

2、若存在相关声明，查看APP功能页面中是否对个性化相关功能、栏目、板块、页面进行显著提示及区分

3、若未进行提示，则判断此项存在问题

未提供关闭选项:

APP 以个人信息处理规则弹窗等形式明示存在定向推送功能，未提供便捷有效的退出或关闭个性化展示模式的选项，如拒绝接受定向推送信息，或停止、退出、关闭相应功能的机制

检测结果 未发现问题