OPPO安全隐私自动化检测报告

应用名称	手机字号一键放大
包名	com.zitifoae4.quanwei
版本	1.1.0
文件类型	Android
MD5	3fb8e656f105fc5854c571b8b27757cf
扫描时间	2025-11-26 11:42:31

OPPO 安全
OPPO Security

目录

声明

本次评估由OPPO安全与隐私部门根据相关法律法规及测评规范对APP进行的隐私自动化检测服务。借助自研的自动化检测工具，对潜在隐私不合规行为进行检测。使用时需注意：

1.为了保证检测结果的完整性，请上传未加固的检测包，以便在测试机上顺利运行。

2.本技术检测报告仅限提示开发者该被检测APP可能的隐私风险，不构成法律意见。未经授权，请勿将该报告对外传播公布，或用于其他目的。

评估标准

1.《中华人民共和国网络安全法》
2.《信息安全技术 个人信息安全规范》（GB/T 35273-2020）
3.《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)
4.《个人信息安全保护自动化测试平台》
5.《中华人民共和国个人信息保护法》
6.《GB/T 35273-2020 信息安全技术 个人信息安全规范》
7.《App 违法违规收集使用个人信息行为认定方法》国信办秘字〔2019〕191 号

检测详情

一、检测结论

总结论	风险项	安全项	待自测风险项
存在风险	1	39	9

检测项名称	结论
违规收集个人信息	通过
超范围收集个人信息	不通过
违规使用个人信息	通过
强制用户使用定向推送功能	通过
APP强制、频繁、过度索取权限	通过
APP不应频繁自启动和关联启动	通过
欺骗误导用户方面	通过

二、检测详情

1.违规收集个人信息

【监管要求】重点整治APP、SDK未告知用户收集个人信息的目的、方式、范围且未经用户同意，私自收集用户个人信息的行为。

检测标准	违规收集个人信息
是否通过	通过

1.1 APP 未以个人信息处理规则弹窗等形式向用户明示个人信息处理的目的、方式和范围，存在收集 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。

检测结果：通过

证据截图：(无)

1.2 APP 以个人信息处理规则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，存在收集 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。

检测结果：通过

证据截图：(无)

1.3 APP 以个人信息处理规则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、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、音视频等个人信息的目的、方式和范围，用户同意后，存在收集相应个人信息。

检测结果：通过

证据截图：(无)

1.4 APP 以个人信息处理规则弹窗等形式向用户明示个人信息处理的目的、方式和范围，未清晰明示在静默状态下或在后台运行时收集个人信息的目的、方式和范围，存在收集相应个人信息。

检测结果：**未评估，可能存在风险，请开发者自评**

自评建议：

第一步：打开APP，等待隐私政策弹窗出现，查看全文

第二步：查看隐私政策中，是否有清晰说明在静默状态下或在后台运行时，用户个人信息的处理目的、方式、范围等

第三步：若未清晰明示在静默状态下或在后台运行时个人信息处理规则，就存在收集个人信息行为，可判定为存在问题

1.5 APP 未以个人信息处理规则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存在收集 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。

检测结果：通过

证据截图：(无)

1.6 APP 以个人信息处理规则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存在收集 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。

检测结果：通过

证据截图：(无)

1.7 APP 以个人信息处理规则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、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、音视频等个人信息的目的、方式和范围，用户同意后，第三方 SDK 存在收集相应个人信息。

检测结果：通过

证据截图：(无)

1.8 APP 以个人信息处理规则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，未清晰明示在静默状态下或在后台运行时第三方SDK收集个人信息的目的、 方式和范围，第三方 SDK 存在收集相应个人信息。

检测结果：**未评估，可能存在风险，请开发者自评**

自评建议：

第一步：打开APP，等待隐私政策弹窗出现，查看全文

第二步：查看隐私政策中，是否有清晰说明在静默状态下或在后台运行时，第三方SDK对用户个人信息的处理目的、方式、范围等

第三步：若未清晰明示在静默状态下或在后台运行时，第三方SDK对个人信息处理规则，就存在收集个人信息行为，可判定为存在问题

1.9 APP 在征求用户同意环节，未提供明确的同意和拒绝选项，使用“好的”、“我知道了”等 无法清晰表达用户同意的词语。

检测结果：通过

证据截图：(无)

1.10 APP 在征求用户同意环节，设置为默认同意（如默认勾选、15S后自动同意等）

检测结果：通过

证据截图：(无)

2.超范围收集个人信息

【监管要求】重点整治APP、SDK非服务所必需或无合理应用场景，特别是在静默状态下或在后台运行时，超范围收集个人信息的行为。

检测标准	超范围收集个人信息
是否通过	不通过

2.1 APP 在收集 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、音视频等个人信息时，超出其所明示收集目的的合理关联范围。

检测结果：通过

证据截图：(无)

2.2 APP 未向用户明示收集 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、音视频等个人信息的频率，未经用户同意，存在以特定频率收集个人信息。

检测结果：通过

证据截图：(无)

2.3 APP 向用户明示收集 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、音视频等个人信息的频率，收集个人信息的频率超出其实现产品或服务的业务功能所必需的最低频率。

检测结果：通过

证据截图：(无)

2.4 APP 向用户明示第三方 SDK 处理 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、音视频等个人信息的目的、方式和范围，第三方SDK收集相应个人信息时，超出其所明示收集目的的合理关联范围。

检测结果：通过

证据截图：(无)

2.5 APP 未向用户明示第三方 SDK收集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、音视频等个人信息的频率，未经用户同意，第三方SDK以特定频率收集个人信息。

检测结果：不通过

检测详情：(1)第三方SDK以特定频率、超频次获取相关信息或者APP首次运行时，未到相关服务和场景提前收集相关信息

改进建议：第三方SDK不应频繁或者超频次获取相关信息，需要到相关服务和场景，在合理范围内进行收集。

证据截图：(无)

2.6 APP 向用户明示第三方 SDK 收集使用 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、音视频等个人信息的频率，第三方SDK收集个人信息的频率超出其实现产品或服务的业务功能所必需的最低频率。

检测结果：通过

证据截图：(无)

2.7 APP 在静默状态下或在后台运行时，收集 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，超出其所明示的收集目的的合理关联范围

检测结果：**未评估，可能存在风险，请开发者自评**

自评建议：

第一步：根据APP内明示要收集个人信息的清单，确定个人信息收集范围

第二步：查看APP在静默状态下或在后台运行时，实际收集个人信息时是否超出必要信息范围
第三步：若存在超范围收集个人信息，则可判定此项存在问题

2.8 APP 未向用户明示在静默状态下或在后台运行时收集 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、音视频等个人信息的频率， 未经用户同意，以特定频次收集个人信息。

检测结果：通过

证据截图：(无)

2.9 APP 向用户明示在静默状态下或在后台运行时收集 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、音视频等个人信息的频率，收集个人信息的频率超出其实现产品或服务的业务功能所必需的最低频率。

检测结果：通过

证据截图：(无)

2.10 APP 在静默状态下或在后台运行时，第三方SDK 收集 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，超出其所明示的收集目的的合理关联范围。

检测结果：**未评估，可能存在风险，请开发者自评**
自评建议：
第一步：根据APP内明示第三方SDK要收集个人信息的清单，确定个人信息收集范围
第二步：查看APP在静默状态下或在后台运行时，第三方SDK实际收集个人信息时是否超出必要信息范围
第三步：若存在超范围收集个人信息，则可判定此项存在问题

2.11 APP 未向用户明示在静默状态下或在后台运行时第三方 SDK 收集 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 信息的频率，未经用户同意，在静默状态下或在后台运行时，第三方SDK以特定频次收集个人信息

检测结果：通过

证据截图：(无)

2.12 APP 向用户明示在静默状态下或在后台运行时第三方 SDK 收集 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、音视频等个人信息的频率，在静默状态或在后台运行时，第三方SDK收集个人信息的频率，超出其实现产品或服务的业务功能所必需的最低频率。

检测结果：通过

证据截图：(无)

3.违规使用个人信息

【监管要求】重点整治APP、SDK未向用户告知且未经用户同意，私自使用个人信息，将用户个人信息用于其提供服务之外的目的，特别是私自向其他应用或服务器发送、共享用户个人信息的行为。

检测标准	违规使用个人信息
是否通过	通过

3.1 APP未向用户明示个人信息处理的目的、方式和范围，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：通过

证据截图：(无)

3.2 APP以个人信息处理规则弹窗等形式向用户明示共享给第三方的行为，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：通过

证据截图：(无)

3.3 APP以个人信息处理规则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：人工自评

证据截图：（无）

4.强制用户使用定向推送功能

【监管要求】重点整治APP、SDK未以显著方式标示且未经用户同意，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，且未提供关闭该功能选项的行为。

检测标准	强制用户使用定向推送功能
是否通过	通过

4.1 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：通过

证据截图：（无）

4.2 APP定向推送功能使用了第三方的个人信息来源，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第三方的个人信息进行定向推送，并向用户明示第三方的个人信息来源。

检测结果：**未评估，可能存在风险，请开发者自评**

自评建议：

第一步：查看APP是否存在定向推送功能

第二步：APP内是否有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

第三步：是否向用户明示第三方的个人信息来源

第四步：若存在定向推送功能且无明示推送个人信息来源，则可判定为存在问题

4.3 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：**未评估，可能存在风险，请开发者自评**

自评建议：

第一步：查看APP是否存在定向推送功能

第二步：APP内是否有弹窗等形式向用户明示存在定向推送功能

第三步：页面中未显著区分定向推送服务，显著方式包括但不限于：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

第四步：若未明示定推规则，且页面未清晰标识定推模块，可判定此项为存在问题

4.4 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：**未评估，可能存在风险，请开发者自评**

自评建议：

第一步：查看APP是否存在定向推送功能

第二步：APP内是否有弹窗等形式向用户明示存在定向推送功能

第三步：页面是否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

第四步：若未提供清晰的关闭选项，可判定此项为存在问题

5.APP强制、频繁、过度索取权限

【监管要求】重点整治APP安装、运行和使用相关功能时，非服务所必需或无合理应用场景下，用户拒绝相关授权申请后，应用自动退出或关闭的行为。重点整治短时长、高频次，在用户明确拒绝权限申请后，频繁弹窗、反复申请与当前服务场景无关权限的行为。重点整治未及时明确告知用户索取权限的目的和用途，提前申请超出其业务功能等权限的行为。

检测标准	APP强制、频繁、过度索取权限
是否通过	通过

5.1 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。

检测结果：通过

证据截图：(无)

5.2 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 循环弹窗申请权限，使用户无法继续使用。

检测结果：通过

证据截图：(无)

5.3 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，APP无法正常注册或登录。

检测结果：通过

证据截图：(无)

5.4 APP 运行时，在用户明确拒绝通讯录、定位、短信、录音、相机、日历等权限申请后，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：通过

证据截图：(无)

5.5 APP 在用户明确拒绝通讯录、定位、短信、录音、相机、日历等权限申请后，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：通过

证据截图：(无)

5.6 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、日历等权限。

检测结果：通过

证据截图：(无)

5.7 APP 未见提供相关业务功能或服务，申请通讯录、定位、短信、录音、相机、日历等权限。

检测结果：通过

证据截图：(无)

6.APP不应频繁自启动和关联启动

【监管要求】重点整治APP未向用户告知且未经用户同意，或无合理的使用场景，频繁自启动或关联启动第三方APP的行为。

检测标准	APP不应频繁自启动和关联启动
是否通过	通过

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

检测结果：通过

证据截图：(无)

6.2 APP向用户明示但未经用户同意，存在自启动或关联启动第其他APP。

检测结果：通过

证据截图：(无)

6.3 APP非服务所必需或无合理应用场景，存在自启动或关联启动其他APP。

检测结果：通过

证据截图：(无)

6.4 SDK非服务所必需或无合理应用场景，存在启动或关联启动APP。

检测结果：**未评估，可能存在风险，请开发者自评**

自评建议：
第一步：查看SDK的服务内容
第二步：查看SDK是否有自启动或关联启动其他APP的行为
第三步：若存在SDK超范围启动或关联启动APP的行为，此项可判定为存在问题

7.欺骗误导用户方面

【监管要求】重点治理APP信息窗口关不掉、欺骗误导强迫下载、安装、使用APP和欺骗误导强迫点击跳转，出现上述任意一种行为，则判定为欺骗误导强迫行为。

检测标准	无欺骗误导用户行为
是否通过	通过

7.1 APP 广告页面、开屏广告、主屏等功能页面，无显著APP下载提示，点击即自动下载非用户所自愿下载APP。

检测结果：通过 证据截图：(无)

7.2 APP 广告页面、开屏广告、主屏等功能页面，以“是否立即开始游戏”方式欺骗误导用户自动下载非用户所自愿下载APP。

检测结果：通过 证据截图：(无)

7.3 APP 广告页面、开屏广告、主屏等功能页面，以“领取红包”方式欺骗误导用户自动下载非用户所自愿下载APP。

检测结果：通过 证据截图：(无)

7.4 APP 广告页面、开屏广告、主屏等功能页面，点击“下载按钮“以外区域，自动下载非用户所自愿下载APP。

检测结果：通过

证据截图：(无)

7.5 暂停下载非用户所自愿下载APP，关闭并重新运行本APP后，自动恢复下载被暂停的非用户所自愿下载的APP。

检测结果：通过

证据截图：(无)

7.6 APP 广告页面、开屏广告、主屏等功能页面，通过设置关闭障碍等方式欺骗误导强迫下载非用户所自愿下载APP。

检测结果：通过

证据截图：(无)

7.7 APP 广告页面、开屏广告、主屏等功能页面，下载的APP与向用户所作的宣传或者承诺不符。

检测结果：通过

证据截图：(无)

7.8 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：通过

证据截图：(无)

7.9 非服务所必需或无合理场景，通过积分、奖励、优惠等方式欺骗误导用户提供身份证号码以及个人生物特征信息的行为。

检测结果：通过

证据截图：(无)

三、待自测风险说明

1、为什么存在自测检测项目？

按照法规和条例，其中要求使用自动化方式现阶段还无法完全实现，所以需要开发者依据法规要求进行自查，也可以让有经验的安全人员，人工进行检测。

2、未完成待自测风险项自评会存在什么风险？

检测报告中的检测项，都是需要关注的点，包括自评项，如果出现问题，都会被通知整改，开发者有自查的义务，需要对本身APP中的隐私问题进行自查和整改，如果不清楚如何排查待自测风险项，可以找隐私安全专业的人协助。