APP 违法违规收集使用个人信息行为认定报告

应用名称：每日英语阅读

应用版本：10.7.4

评估时间：2023-11-29

评估机构：捷兴信源

目　　录

声　明

本次评估由捷兴信源《个人信息安全保护自动化测试平台》依据《中华人民共和国个人信息保护法》、《GB/T 35273-2020 信息安全技术 个人信息安全规范》、《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、《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）》等相关规范对 APP 进行深度评估得出，仅用于帮助您发现 APP 中可能存在的个人信息安全问题。

捷兴信源具备完善的APP个人信息安全检测与技术实践能力。基于真机的行为监控沙箱，提供了全接口监控能力和网络报文实时监控能力；结合资深专业测试人员依据覆盖最为全面的测试用例开展专业化深度测试；评估覆盖APP前端、后台、静默等多个不同场景。切实保障了应用个人信息安全风险检测的专业性和全面性。

如您存有检测结果疑问或寻求政策解读、详细整改方案咨询等方面的专业辅导需求，可联系我司为您进行深度检测服务，**深度检测服务可覆盖工信部《关于开展纵深推进 APP 侵害用户权益专项整治行动的通知》（164 号文）的所有检测项，完全符合标准要求。**

检 测 依 据

- 《中华人民共和国网络安全法》
- 《中华人民共和国个人信息保护法》
- 《中华人民共和国消费者权益保护法》
- 《GB/T 35273-2020 信息安全技术 个人信息安全规范》
- 《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
- 《信息安全技术移动互联网应用程序（APP）收集个人信息基本规范（征求意见稿）》
- 《工信部 App 侵害用户权益专项整治 8 项要求（工信部信管函（2019）337 号） 》
- 《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）》
- 《个人信息出境安全评估办法（征求意见稿）》
- 《儿童个人信息网络保护规定》
- 《网络安全标准实践指南移动互联网应用程序（APP）手机使用个人信息自评估指南》
- 《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》
- 《网络安全标准实践指南移动互联网应用程序（APP）使用软件开发工具包（SDK）安全指导》
- 《TTAF 077.1-2020 APP 收集使用个人信息最小必要评估规范》
- 《TTAF 065-2020 移动智能终端与应用软件用户个人信息保护实施指南》
- 《TTAF 078.1-2020 APP 用户权益保护测评规范》

一、 检测结论

本次检测依据《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》）中提出的四个方面、十类问题、44 个检测细则进行评估， 其中通过检测 9 项，未通过 4 项，需人工检测 31 项。

检测项名称	检测内容	检测结果
APP、SDK 违规处理用户个人信息方面	违规收集个人信息	不通过
	超范围收集个人信息	不通过
	违规使用个人信息	需人工检测
	强制用户使用定向推送功能	需人工检测
设置障碍、频繁骚扰用户方面	APP 强制、频繁、过度索取权限	通过
	APP 频繁自启动和关联启动	需人工检测
欺骗误导用户方面	欺骗误导强迫用户	需人工检测
	欺骗误导用户提供个人信息	需人工检测
应用分发平台责任落实不到位方面	应用分发平台上的 APP 信息明示不到位	需人工检测
	应用分发平台管理责任落实不到位	需人工检测

■ 结果说明：

“不通过”指 APP 在自动化检测环境的测试场景中存有不合格项，请根据检测结果自查自改。

“通过”指 APP 在自动化检测环境的测试场景中未发现不合格项，但受自动化测试场景限制，该结构可能存有遗漏和偏差，建议根据相关要求进一步深度自查。

“需人工检测”指 APP 不具备自动化检测环境，无法开展测试，建议根据相关要求进一步深度自查。

二、 APP 违法违规收集使用个人信息行为认定结果

■ APP 收集使用个人信息评测-基础信息

软件名称	每日英语阅读
软件版本	10.7.4
安装包 MD5	c9f0981ba3c6888fe993affe1152d4c1
分析时间	2023-11-29

■ App 违法违规收集使用个人信息行为认定评估结果

评估方面（一） APP、SDK 违规处理用户个人信息方面

依据规范： 《个人信息保护法》第七条 处理个人信息应当遵循公开、透明原则，公开个人信息处理规则，明示处理的目的、方式和范围。

第一类问题：违规收集个人信息

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。

测试场景一：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 IMEI、IMSI、设备 MAC 地址、应用安装列表、通讯录、通话记录、短信的行为。

- 检测结果： 通过
- 结果说明： 自动化检测未发现问题，建议采用人工深度测试进一步自查复核
- 自查建议：

App 首次运行时应该通过弹窗等明显方式提示用户阅读隐私政策等收集使用规则，个人信息保护政策应该逐一列出 App 收集使用个人信息的目的、方式、范围等规则，且在征得用户明确表示同意前，不要收集用户个人信息。

测试场景二：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 IMEI、IMSI、设备 MAC 地址、应用安装列表、通讯录、通话记录、短信的行为。

- 检测结果：不通过
- 结果说明：APP 存在未经用户同意读取“硬件序列号”的行为
- 自查建议：

App 首次运行时应该通过弹窗等明显方式提示用户阅读隐私政策等收集使用规则；个人信息保护政策应该逐一列出 App 收集使用个人信息的目的、方式、范围等内容；且建议在征得用户明确表示同意前，不要收集用户个人信息。

测试场景三：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 收集设备 MAC 地址、应用安装列表等的目的方式范围，用户同意隐私政策后，存在收集设备 MAC 地址、应用安装列表的行为。

- 检测结果：未测试
- 结果说明：受自动化测试条件限制，未开展该项检查，建议采用人工深度测试进一步自查复核
- 自查建议：

App 首次运行时应该通过弹窗等明显方式提示用户阅读隐私政策等收集使用规则；个人信息保护政策应该逐一列出 App 收集使用个人信息的目的、方式、范围等内容，请勿有所遗漏；且建议在征得用户明确表示同意前，不要收集用户个人信息。

测试场景四：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 IMEI、IMSI、设备 MAC 地址和应用安装列表、通讯录和短信的行为。

- 检测结果：不通过
- 结果说明：存在若干 SDK 未经用户许可读取个人隐私信息（硬件序列号）
- 自查建议：

App 首次运行时应该通过弹窗等明显方式提示用户阅读隐私政策等收集使用规则；个人信息保护政策应该逐一列出 App 中嵌入的全部 SDK 及各 SDK 收集使用个人信息的目的、方式、范围等内容；且建议在征得用户明确表示同意前，SDK 不要收集用户个人信息。

测试场景五：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 IMEI、设备 MAC 地址和应用安装列表、通讯录、通话记录、和短信的行为。

- 检测结果： 不通过
- 结果说明： 存在若干 SDK 未经用户许可读取个人隐私信息（硬件序列号）
- 自查建议：

App 首次运行时应该通过弹窗等明显方式提示用户阅读隐私政策等收集使用规则；个人信息保护政策应该逐一列出 App 中嵌入的全部 SDK 及各 SDK 收集使用个人信息的目的、方式、范围等内容；且建议在征得用户明确表示同意前，SDK 不要收集用户个人信息。

测试场景六：APP 向用户明示 SDK 的收集使用规则，但未见清晰明示 SDK 收集设备 MAC 地址、应用安装列表等的目的方式范围，用户同意隐私政策后，SDK 存在收集设备 MAC 地址、应用安装列表的行为。

- 检测结果：未测试
- 结果说明：受自动化测试条件限制，未开展该项检查，建议采用人工深度测试进一步自查复核
- 自查建议

App 首次运行时应该通过弹窗等明显方式提示用户阅读隐私政策等收集使用规则；个人信息保护政策应该逐一列出 App 中嵌入的全部 SDK 及各 SDK 收集使用个人信息的目的、方式、范围等内容，请勿有所遗漏；且建议在征得用户明确表示同意前，SDK 不要收集用户个人信息。

测试场景七：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。

- 检测结果： 通过
- 结果说明： 自动化检测未发现问题，建议采用人工深度测试进一步自查复核
- 自查建议：

APP 在征求用户同意环节，应提供明确的同意或拒绝按钮，不建议使用“好的”“我知道了”等模棱两可，语义不明的词语。

测试场景八：App 在征求用户同意环节，设置为默认勾选。

- 检测结果：未测试。

- 结果说明：受自动化测试条件限制，未开展该项检查，建议采用人工深度测试。
- 自查建议：

App 应把用户自主作出的肯定性动作，如主动点击、勾选、填写等，作为产品或服务的特定业务功能的开启条件，在用户注册登录或者阅读隐私政策等收集使用规则时，不建议默认勾选表示同意。

第二类问题：超范围收集个人信息

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。

测试场景一：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。

- 检测结果：未测试
- 结果说明：受自动化测试条件限制，未开展该项检查，建议采用人工深度测试
- 自查建议：

APP 收集的个人信息的类型应与实现其业务功能有直接关联；不建议未见向用户告知且未经用户同意、在非服务所必需且无合理应用场景的情况下收集使用个人信息；可通过功能验证、技术检测等手段核查 APP 实际收集的个人信息是否与业务功能有直接关联。

测试场景二：APP 在运行时，未见向用户告知且未经用户同意，存在每 30s 读取一次位置信息，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。

- 检测结果：未测试
- 结果说明：受自动化测试条件限制，未开展该项检查，建议采用人工深度测试
- 自查建议：

APP 自动采集个人信息的频率应是实现 APP 的业务功能所必需的最低频率；不建议非服务所必需且无合理应用场景的情况下，超出实现产品或服务的业务功能所必需的最低频率收集个人信息；可通过功能验证、技术检测查看 APP 是否存在频繁收集个人信息的行为。

测试场景三：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。

- 检测结果：未测试
- 结果说明：受自动化测试条件限制，未开展该项检查，建议采用人工深度测试
- 自查建议：

APP 中嵌入的 SDK 收集使用个人信息，应与实现其业务功能有直接关联；不建议 SDK 未见向用户告知且未经用户同意、在非服务所必需且无合理应用场景的情况下收集个人信息；可通过功能验证、技术检测

查看 SDK 实际收集的个人信息是否与业务功能有直接关联。

测试场景四：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 读取一次位置信息，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。

- 检测结果：未测试
- 结果说明：受自动化测试条件限制，未开展该项检查，建议采用人工深度测试
- 自查建议：

APP 中嵌入的 SDK 收集使用个人信息的频率应是实现其业务功能所必需的最低频率；可通过功能验证、技术检测等手段核查 SDK 收集使用个人信息的频率，并结合 SDK 实际功能，判断 SDK 自动收集个人信息的频率是否是实现其业务功能所必需的最低频率。

测试场景五：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。

- 检测结果：未测试
- 结果说明：受自动化测试条件限制，未开展该项检查，建议采用人工深度测试
- 自查建议：

APP 收集使用个人信息应与实现其业务功能有直接关联；不建议未经用户许可，在静默状态下或在后台运行时、无合理场景获取个人信息。可通过功能验证、技术检测方式验证 APP 在静默状态下或后台运行时的收集使用个人信息行为。

测试场景六：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。

- 检测结果：通过
- 结果说明：自动化检测未发现问题，建议采用人工深度测试进一步自查复核
- 自查建议：

APP 收集使用个人信息应与实现其业务功能有直接关联，且采集的频率应是实现 APP 的业务功能所必需的最低频率；不建议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，按照一定频次收集个人信息。可通过功能验证，技术检测等方法核验 APP 前台、后台和静默运行时自动收集个人信息的频率研判是否超出业务功能所必需的最低频率。

测试场景七：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。

- 检测结果：不通过
- 结果说明：非服务所必需,存在若干 SDK 未经用户许可读取个人隐私信息（硬件序列号）

- 自查建议：

APP 中嵌入的 SDK 收集使用个人信息应与实现其业务功能有直接关联；不建议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，收集收集个人信息。可通过功能验证、技术检测查看 SDK 在静默状态下或在后台运行时，是否与业务功能有无关的个人信息。

测试场景八：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。

- 检测结果：未测试
- 结果说明：受自动化测试条件限制，未开展该项检查，建议采用人工深度测试
- 自查建议：

APP 中嵌入的 SDK 收集使用个人信息的频率应是实现其业务功能所必需的最低频率；不建议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，SDK 按照一定频次收集与功能无关的个人信息。可通过功能验证、技术检测等手段，核验 SDK 在 APP 后台和静默运行时，SDK 自动收集个人信息的频率，并结合 SDK 提供者提业务场景，判断 APP 中 SDK 自动收集个人信息的频率是否是实现其业务功能所必需的最低频率。

第三类问题：违规使用个人信息

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。

测试场景一：APP 未见向用户告知且未经用户同意，存在将 IMEI/设备 MAC 地址/应用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。

- 检测结果：未测试。
- 结果说明：受自动化测试条件限制，未开展该项检查，建议采用人工深度测试进一步自查复核。
- 自查建议：

App 向第三方共享个人信息时，不应超出与收集个人信息时所声称的目的范围。因业务需要，确需向第三方共享时，应在隐私政策中明确告知，并征得用户同意；不建议未经用户许可向第三方传输用户个人信息。可通过功能验证、技术检测等方式核验是否存在未经用户许可向第三方共享个人信息的行为。

测试场景二：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，存在将“设备 MAC 地址”个人信息发送给友盟第三方 SDK 的行为。

- 检测结果：未测试
- 结果说明：受自动化测试条件限制，未开展该项检查，建议采用人工深度测试进一步自查复核
- 自查建议：

App 向第三方共享个人信息时，不应超出与收集个人信息时所声称的目的范围。因业务需要，确需向

第三方共享时，应在隐私政策中明确告知，并征得用户同意；不建议未经用户许可向第三方传输用户个人信息。可通过功能验证、技术检测等方式核验是否存在未经用户许可向第三方共享个人信息的行为。

测试场景三：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/应用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。

- 检测结果：未测试
- 结果说明：受自动化测试条件限制，未开展该项检查，建议采用人工深度测试进一步自查复核
- 自查建议：

App 向第三方共享个人信息时，不应超出与收集个人信息时所声称的目的范围。因业务需要，确需向第三方共享时，应在隐私政策中明确告知，并征得用户同意；不建议未经用户许可向第三方传输用户个人信息。可通过功能验证、技术检测等方式核验是否存在未经用户许可向第三方共享个人信息的行为。

第四类问题：强制用户使用定向推送功能

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。

测试场景一：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。

- 检测结果：未测试。
- 结果说明：受自动化测试条件限制，未开展该项检查，建议采用人工深度测试进一步自查复核。
- 自查建议：

App 提供者在向用户提供业务功能的过程中使用个性化展示的，应在隐私政策中以显著的方式告知用户将收集的个人信息用作定向推送等个性化展示。

测试场景二：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。

- 检测结果：未测试
- 结果说明：受自动化测试条件限制，未开展该项检查，建议采用人工深度测试进一步自查复核。
- 自查建议：

App 提供者在向用户提供业务功能的过程中使用个性化展示的，应显著区分个性化展示的内容和非个性化展示的内容，可核验 App 是否向用户同时提供包含个性化展示和非个性化展示的业务功能；查看当 App 提供的业务功能使用个性化展示时，是否通过标注“定推、推荐、关注、猜你喜欢”等字样显著区分个性化展示和非个性化展示的内容；或通过不同的栏目、板块、页面等显著区分个性化展示和非个性化展示内容；以及是否提供非定向推送信息的选项。

测试场景三：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，

但未见提供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：未测试
- 结果说明：受自动化测试条件限制，未开展该项检查，建议采用人工深度测试进一步自查复核
- 自查建议：

App 提供者在向用户提供业务功能的过程中使用个性化展示的，应为用户提供退出或关闭个性化展示模式的选项，包括向用户提供不针对其个人特征的选项；为用户提供简单直观的退出或关闭个性化展示模式的选项；当用户选择退出或关闭个性化展示模式时，应向用户提供删除或匿名化定向推送活动所基于的个人信息的选项。

评估方面（二） 设置障碍、频繁骚扰用户方面

依据规范： 《个人信息保护法》 第十四条 基于个人同意处理个人信息的，该同意应当由个人在充分知情的前提下自愿、明确作出。

第五类问题：APP 强制、频繁、过度索取权限

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。

测试场景一：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）。

- 检测结果： 通过
- 结果说明： 自动化检测未发现问题，建议采用人工深度测试进一步自查复核
- 自查建议：

App 首次启动时，向用户索取收集个人信息的权限，应同步告知打开可收集个人信息的目的，在用户明确表示不同意后，不应该退出、关闭或频繁征求用户同意、干扰用户正常使用。

测试场景二：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。

- 检测结果：通过
- 结果说明：自动化检测未发现问题，建议采用人工深度测试进一步自查复核
- 自查建议：

App 运行时，应该在服务所必须的合理场景下向用户索取收集个人信息的权限，并同步告知打开可收集个人信息的目的，在用户明确表示拒绝后，不应该退出、关闭干扰用户正常使用。

测试场景三：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。

- 检测结果：未测试
- 结果说明：受自动化测试条件限制，未开展该项检查，建议采用人工深度测试进一步自查复核
- 自查建议：

App 在用户注册登录场景时，向用户索取收集个人信息的权限，在用户明确表示拒绝后，不应该拒绝用户正常使用注册或登录功能。

测试场景四：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）。

- 检测结果：未测试
- 结果说明：受自动化测试条件限制，未开展该项检查，建议采用人工深度测试进一步自查复核
- 自查建议：

App 运行时，应该在服务所必须的合理场景下向用户索取收集个人信息的权限，并同步告知打开可收集个人信息的目的，在用户明确表示拒绝后，不应该退出、关闭或频繁征求用户同意、干扰用户正常使用。

测试场景五：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。

- 检测结果：通过
- 结果说明：自动化检测未发现问题，建议采用人工深度测试进一步自查复核
- 自查建议：

App 运行时，应该在服务所必须的合理场景下向用户索取收集个人信息的权限，并同步告知打开可收集个人信息的目的，在用户明确表示拒绝后，不应该频繁征求用户同意、干扰用户正常使用。

测试场景六：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。

- 检测结果： 通过
- 结果说明： 自动化检测未发现问题，建议采用人工深度测试进一步自查复核
- 自查建议：

App 运行时，应该在服务所必须的合理场景下向用户索取收集个人信息的权限，并同步告知打开可收集个人信息的目的，在用户明确表示拒绝后，重新运行时，不应再次弹窗申请与当前服务场景无关的权限，干扰用户正常使用。

测试场景七：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。

- 检测结果：通过

- 结果说明：自动化检测未发现问题，建议采用人工深度测试进一步自查复核
- 自查建议：

APP 不应在打开时一次性连续弹窗要求用户授权当前还未使用的业务功能所需的权限。

测试场景八：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/XXX 等权限。

- 检测结果：通过
- 结果说明：自动化检测未发现问题，建议采用人工深度测试进一步自查复核
- 自查建议：

用户未使用 App 某项业务功能的某项特定功能时，不应要求用户授权相应权限。

第六类问题：APP 频繁自启动和关联启动

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。

测试场景一：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。

- 检测结果：未测试
- 结果说明：受自动化测试条件限制，未开展该项检查，建议采用人工深度测试进一步自查复核
- 自查建议：

APP 在未向用户告知且未经用户同意，或无合理的使用场景时，不应频繁自启动或关联启动第三方 APP 并收集个人信息；可查看 APP 的隐私政策中是否说明 APP 具有自启动或关联启动第三方 APP 并收集个人信息的行为；通过技术检测查看 APP 是否存在自启动并在自启动后收集个人信息的行为；查看 APP 在使用或静默状态是否存在关联启动第三方 APP 并收集个人信息的行为；结合 APP 提供者提供的证明材料，判断 APP 自启动或关联启动第三方 APP 并收集个人信息的行为是否合理。

测试场景二：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。

- 检测结果：未测试
- 结果说明：受自动化测试条件限制，未开展该项检查，建议采用人工深度测试进一步自查复核
- 自查建议

当 APP 通过隐私政策向用户告知自启动或关联启动的目的时，不应在用户同意隐私政策前，频繁自启动或关联启动第三方 APP 并收集个人信息；可查看 APP 的隐私政策中是否说明 APP 具有自启动或关联启动的合理业务场景；通过功能验证、技术检测等方式查看 APP 是否同意隐私政策前，自启动或关联启动。

测试场景三：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。

- 检测结果：未测试

- 结果说明：受自动化测试条件限制，未开展该项检查，建议采用人工深度测试进一步自查复核
- 自查建议：

APP 不应在无合理的使用场景时，频繁自启动或关联启动，可查看 APP 的隐私政策中是否说明 APP 自启动或关联启动的合理场景，并通过功能验证、技术检测等手段核验 APP 是否存在自启动或关联启动行为。

评估方面（三） 欺骗误导用户方面

依据规范： 《个人信息保护法》第五条 处理个人信息应当遵循合法、正当、必要和诚信原则，不得通过误导、欺诈、胁迫等方式处理个人信息。

第七类问题：欺骗误导强迫用户

重点整治通过“偷梁换柱”“移花接木”等方式欺骗误导用户下载 APP，特别是具有分发功能的移动应用程序欺骗误导用户下载非用户所自愿下载 APP 的行为。

测试场景一：APP 广告未向用户提供关闭或退出窗口的标识、未以显著的方式向用户提供关闭或退出窗口的标识、或广告向用户提供关闭或退出窗口的标识，但存在虚假或无效。

- 检测结果：未测试
- 结果说明：受自动化测试条件限制，未开展该项检查，建议采用人工深度测试进一步自查复核
- 自查建议：

APP 中不应存在欺诈、诱骗、误导用户的行为，APP 广告页面、开屏广告、激励广告等信息窗口，应以显著方式提供真实有效的关闭或退出窗口的标识。

测试场景二：APP 开屏页信息窗口未见显著提示，用户点击该页面后即进入到信息窗口页面或者第三方应用下载页面等。

- 检测结果：未测试
- 结果说明：受自动化测试条件限制，未开展该项检查，建议采用人工深度测试进一步自查复核
- 自查建议：

APP 中不应存在欺诈、诱骗、误导用户的行为，APP 开屏页信息窗口应提供显著提示信息，以及真实有效合理的进入到信息窗口页面或者第三方应用下载页面方式。

测试场景三：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 所自愿下载的 APP。

- 检测结果：未测试
- 结果说明：受自动化测试条件限制，未开展该项检查，建议采用人工深度测试进一步自查复核
- 自查建议：

APP 中不应存在欺诈、诱骗、误导用户的行为，在 APP 广告页面、开屏广告、主屏等功能页面分发 APP 时，下载按钮以外区域，不得提供下载或跳转功能。

测试场景四：用户暂停或取消非主动点击触发下载的 APP，关闭并重新运行本 APP 后，被用户暂停或取消下载的 APP 自动恢复下载。

- 检测结果：未测试
- 结果说明：受自动化测试条件限制，未开展该项检查，建议采用人工深度测试进一步自查复核
- 自查建议：

APP 中不应存在欺诈、诱骗、误导用户的行为，重新运行时，不应该恢复下载用户主动暂停或取消下载的 APP。

测试场景五：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：未测试
- 结果说明：受自动化测试条件限制，未开展该项检查，建议采用人工深度测试进一步自查复核
- 自查建议：

APP 中不应存在欺诈、诱骗、误导用户的行为，在 APP 广告页面、开屏广告、主屏等功能页面分发 APP 时，不应该设置关闭障碍欺骗误导强迫用户下载。

测试场景六：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：未测试
- 结果说明：受自动化测试条件限制，未开展该项检查，建议采用人工深度测试进一步自查复核
- 自查建议：

APP 中不应存在欺诈、诱骗、误导用户的行为，在 APP 广告页面、开屏广告、主屏等功能页面分发 APP 时，下载的 APP 应该与向用户宣传或承诺的一致。

第八类问题：欺骗误导用户提供个人信息

重点整治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。

测试场景一：APP 广告页面、开屏广告、主屏等功能页面，存在欺骗误导用户提供身份证号/人脸/指纹等个人信息的行为。

- 检测结果：未测试
- 结果说明：受自动化测试条件限制，未开展该项检查，建议采用人工深度测试进一步自查复核
- 整改建议：

APP 中不应存在以欺诈、诱骗、误导的方式收集个人信息的情况，具体为：

1、APP 隐私政策，是否存在以欺诈、诱骗、误导的方式描述收集个人信息的行为；

2、通过功能验证、技术检测查看 APP 是否存在以欺诈、诱骗、误导的方式收集个人信息的行为。

评估方面（四） 应用分发平台责任落实不到位方面

依据规范： 《移动智能终端应用软件预置和分发管理暂行规定》 第六条 生产企业和互联网信息服务提供者均应明示所提供移动智能终端应用软件相关信息。（一）生产企业和互联网信息服务提供者均应通过用户提示、企业网站等方式明示所提供移动智能终端应用软件的信息，包括名称、功能描述、卸载方法、开发者信息、软件安装及运行所需权限列表等，明确告知用户应用软件收集、使用用户个人信息的内容、目的、方式和范围等。

第九类问题：应用分发平台上的 APP 信息明示不到位

重点整治应用分发平台上未明示 APP 运行所需权限列表及用途，未明示 APP 收集、使用用户个人信息的内容、目的、方式和范围等行为。

测试场景一：APP 具有分发功能，用户通过该 APP 下载第三方 APP 时，未见明示或明示不清晰“应用名称、开发者信息、应用版本号、权限列表及用途、隐私政策”，或明示的与实际不符。

- 检测结果：未测试
- 结果说明：受自动化测试条件限制，未开展该项检查，建议采用人工深度测试进一步自查复核
- 自查建议：

如 APP 涉及分发业务时，应承担分发平台所应承担的分发职责。建议在下载页面显著明示：分发 APP 的名称、版本、安装及运行所需权限列表及用途、收集使用个人信息的内容、目的、方式和范围，相关信息建议真实完整有效，明示 APP 的名称应与下载安装后的 APP 名称一致，且明示不建议隐藏在二级链接。

第十类问题：应用分发平台管理责任落实不到位

重点整治 APP 上架审核不严格、违法违规软件处理不及时和 APP 提供者、运营者、开发者身份信息不真实、联系方式虚假失效等问题。

测试场景一：所分发 APP 的开发者身份信息不真实或不准确。

- 检测结果：未测试。
- 结果说明：受自动化测试条件限制，未开展该项检查，建议采用人工深度测试进一步自查复核。
- 自查建议：

如 APP 涉及分发业务时，应承担分发平台所应承担的分发职责。建议在下载页面显著明示：分发 APP 的名称、版本、安装及运行所需权限列表及用途、收集使用个人信息的内容、目的、方式和范围，相关

信息建议真实完整有效，明示 APP 的名称应与下载安装后的 APP 名称一致，且明示不建议隐藏在二级链接。

测试场景二：所分发 APP 的开发者联系方式失效。

- 检测结果：未测试
- 结果说明：受自动化测试条件限制，未开展该项检查，建议采用人工深度测试进一步自查复核
- 自查建议

如 APP 涉及分发业务时，应承担分发平台所应承担的分发职责。建议在下载页面显著明示：分发 APP 的名称、版本、安装及运行所需权限列表及用途、收集使用个人信息的内容、目的、方式和范围，相关信息建议真实完整有效，明示 APP 的名称应与下载安装后的 APP 名称一致，且明示不建议隐藏在二级链接。

测试场景三：所分发 APP 上架审核不严格、违法违规软件处理不及时。

- 检测结果：未测试
- 结果说明：受自动化测试条件限制，未开展该项检查，建议采用人工深度测试进一步自查复核
- 自查建议：

如 APP 涉及分发业务时，应承担分发平台所应承担的分发职责，对所分发的 APP 进行上架前的严格审核、对违法违规软件进行及时下架处理。

附件一：Android 涉及个人信息权限

序号	权限分组	权限名	功能描述	可访问的个人信息	业务功能示例
1	CAENDAR 日历	READ_CALENDA 读取日历	允许 App 读取用户日历数据	系统日历中的日程安排、备忘、行程等信息	例如日程规划、事件提醒、票务预订等
2		WRITE_CALENDAR 编辑日历	允许 App 写入用户日历数据		
3	CALL_LOG 通话记录	READ_CALL_LO 读取通话记录	允许 App 读取用户通话记录	用户通话记录	例如通话记录管理、备份与恢复，骚扰截、SOS 紧急求助等
4		WRITE_CALL_LOG 编辑通话记录	允许 App 写入用户通话记录		
5		PROCESS_OUTGOING_CALLS 监听呼出电话	允许 App 查看正在拨打的号码，并监听、控制或终止呼出电话	用户呼出的电话号码、呼叫状态等信息	例如呼出电话监控场景、儿童手表、骚扰拦截等
6	CAMERA 相机	CAMERA 拍摄	允许 App 使用摄像头	照片或视频信息	例如拍摄照片视频、扫描二维码/条形码、人脸识别等
7	CONTACTS 通讯录	READ_CONTACTS 读取通讯录	允许 App 读取用户通讯录	联系人数据	例如通讯录管理与备份、添加联系人等
8		WRITE_CONTACTS 编辑通讯录	允许 App 写入用户通讯录		
9		GET_ACCOUNTS 获取 App 账户	允许 App 从账户务中获取 App 账户列表	账户服务中的 App 账户列表	账号登录场景等
10	LOCATION 位置	ACCESS_FINE_LOCATION 访问精准定位	允许 App 获取基于 GPS 等的精准地理位置	精准地理位置信息	例如定位当用户位置、拍照记录照片拍摄位置、社交分享位置、O2O 上门服务定位用户位置等需要用户精准位置的场景
11		ACCESS_COARSE_LOCATION 访问粗略位置	允许 App 获取基于基站、IP 等粗略的地理位置	粗略地理位置信息	例如外卖、本地生活服务等分区域信息推荐、基于城市或地域进行新

					闻推送等基于粗略用户地理置的场景
12		ACCESS_BACKGROUND_LOCATION 支持后台访问位置	允许 App 在后台运行时使用位置信息（需要 App 获得访问粗略位置或访问精准位置权限）	实时地理位置信息、行踪轨迹	例如地图导航、网络约车、运动健身等场景
13	MICROPHONE 麦克风	RECORD_AUDIO 录音	允许 App 使用麦克风进行录音	录音内容	例如语音即时通信、语音识别、音视频录制、直播等语音输入场景
14	PHONE 电话	READ_PHONE_STATE 读取电话状态	App 可通过此权限获取设备 IMSI（国际移动用户识别码）、IMEI（国际移动设备识别码）等设备唯一标识信息，以及手机通话状态等	设备唯一标识信息（如 IMEI、设备序列号）	进行用户常用设备的标识，可用于监测 App 账户异常登录、关联用户行为
15		READ_PHONE_NUMBERS 读取本机电话号码	允许 App 读取用户的本机电话号码	手机号码	读取本机号码场景
16		CALL_PHONE 拨打电话	允许 App 直接拨打电话	实时通话行为	例如在 App 内直接拨打商家、快递员、客服电话等
17		ANSWER_PHONE_CALLS 接听电话	允许 App 接听拨入的电话		例如在驾驶模式下直接接听来电等
18		ADD_VOICEMAIL 添加语音邮件	允许 App 向邮件中添加语音附件	语音邮件内容	
19		USE_SIP 使用网络电话	允许 App 拨打/接听 SIP 网络电话	实时网络通话行为	例如接听、拨打网络电话等
20		ACCEPT_HANDOVER 继续进行来自其他 App 的通话	允许 App 继续进行在其他 App 中发起的通话	实时网络通话行为	
21	BODY_SENSORS 身体传感器	BODY_SENSORS 获取身体传感器信息	允许 App 访问身体内部状况相关的传感器数据，一般特指心率传感器数据	心率等身体传感器数据	例如运动健身、健康类 App 及可穿戴设备显示心率等状况

22	SMS 短信	SEND_SMS 发送短信	允许 App 发送短信	短信	例如短信管理、短信备份恢复、手机号码注册或登录时的验证码场景、SOS 紧急求助等
23		RECEIVE_SMS 接收短信	允许 App 接收短信		
24		READ_SMS 读取文字讯息（短信或彩信）	允许 App 读取短信或彩信	短信、彩信内容	
25		RECEIVE_WAP_PUSH 接收 WAP 推送	允许 App 接收 WAP 推送信息	WAP 推送消息	例如短信管理、WAP 消息推送场景等
26		RECEIVE_MMS 接收彩信	允许 App 接收彩信	彩信	例如短信管理、接收彩信场景等
27	STORAGE 存储	READ_EXTERNAL_STORAGE 读取外置存储器	允许 App 读取外置存储器	外置存储器存储的个人数据	例如文件管理、阅读器等打开本地文件的场景等
28		WRITE_EXTERNAL_STORAGE 写入外置存储器	允许 App 写入外置存储器		例如存储拍摄的照片和视频，及下载文件、需要下载大量资源的游戏场景等
29		ACCESS_MEDIA_LOCATION 读取照片位置信息	允许 App 读取照片文件中包含的拍摄地点信息	照片拍摄地点信息	例如展示照片拍摄地点的场景等
30	ACTIVITY_RECOGNITION 身体活动	ACTIVITY_RECOGNITION 识别身体活动	允许 App 识别身体活动	特定身体活动变化信息（如未移动、步行、跑步、骑车、坐车等）	例如追踪用户步数及卡路里消耗、需要对用户的身体活动进行分类的场景等

附件二：iOS 涉及个人信息权限

序号	受保护的资源	权限名	功能描述	可访问的个人信息
1	Calendar and Reminders 日历与提醒事项	Calendars 日历	访问用户的日历数据	日历数据
2		Reminders 提醒事项	访问用户的提醒事项	提醒事项
3	Camera and Microphone 相机	Camera 相机	访问设备的相机	拍摄的照片与视频

4	与麦克风	Microphone 麦克风	访问设备的麦克风	语音数据
5	Contacts 通讯录	Contacts 通讯录	访问用户的联系人	联系人数据
6	Face ID 面容 ID	FaceID 面容 ID	使用 Face ID 进行身份验证	面容 ID
7	Health 健康	Health Records 健康记 录	读取临床健康记录	临床健康记录
8		Health Share 读取 HealthKit 健康数据	从 HealthKit 存储读取 样本	健康数据
9		Health Update 更新 HealthKit 健康数据	将样本保存到 HealthKit 存储	健康数据
10	Home 家居	HomeKit 家居	请求访问用户的 HomeKit 配置数据	HomeKit 配置数据
11	Location 定位服务	Location Always and When In Use 始终访问 位置	始终访问用户的位置信息	位置信息
12		Location When In Use Usage 使用期间访问位 置	使用 App 期间（前台 运行时）访问用户的 位置信息	位置信息
13	MediaPlayer 媒体与 Apple Music	Media Library 媒体库	访问用户的媒体库	Apple Music、音乐和视频活动以及媒体资料库
14	Motion 运动与健身	Motion 运动与健身	访问设备的加速度计	身体活动、步数统计、已爬楼层数等在内的传感器数据
15	Photos 照片	Photo Library Additions 只写照片库	只写访问用户照片库	照片库
16		Photo Library 读取和写入照片库	读取和写入用户照片库	照片库
17	Speech 语音识别	Speech Recognition 语音识别	使用 Apple 的服务器执行语音识别（将用户数据发送至 Apple 的语音识别服务器）	语音数据

附件三：安卓特殊敏感权限

由于某些特殊用途的 App 功能扩展的需要，安卓系统也提供了一些特殊的敏感权限。这些权限由于涉及到设备、系统、其他 App 的安 全和用户体验，一旦被恶意 App 获取，可能侵犯用户隐私或设备安全，因此，通常只有少数 App 在少数场景才申请，建议提供单独管理界面详细说明申请目的，并适当增加障碍设计避免用户误操作。

序号	权限名	功能描述	业务功能示例
1	BIND_DEVICE_ADMIN 设备管理器	允许 App 激活使用设备管理器	需对设备进行设置才允许在设备上办公的场景
2	BIND_ACCESSIBILITY_SERVICE 辅助模式	也称无障碍功能，允许 App 通过屏幕取词、模拟用户点击等方式，方便 用户操作	无障碍人士使用场景
3	BIND_NOTIFICATION_LISTENER_SERVICE 监听通知栏	允许 App 监听其他 App 通知栏显示的内容	需要将通知栏内容引导到其它设备的场景
4	SYSTEM_ALERT_WINDOW 悬浮窗	允许 App 在其他 App 上覆盖显示	视频聊天、直播软件需要小窗体播放场景；录屏软件、音乐软件等需要悬浮或桌面上显示的场景
5	PACKAGE_USAGE_STATS 读取应用使用情况	允许 App 获取其他 App 的使用统计数据，例如使 用频率、使用时长、语 言设置等使用记录	应用商店、安全管理等需要监控应用的场景

附件四：个人信息

个人信息是指以电子或者其他方式记录的能够单独或者与其他信息结合识别特定自然人身份或者反映特定自然人活动情况的各种信息，如姓名、出生日期、身份证件号码、个人生物识别信息、住址、通信通讯联系方式、通信记录和内容、账号密码、财产信息、征信信息、行踪轨迹、住宿信息、健康生理信息、交易信息等。

判定某项信息是否属于个人信息，应考虑以下两条路径：一是识别，即从信息到个人，由信息本身的特殊性识别出特定自然人，个人信息应有助于识别出特定个人。二是关联，即从个人到信息，如已知特定自然人，由该特定自然人在其活动中产生的信息（如个人位置信息、个人通话记录、个人浏览记录等）即为个人信息。符合上述两种情形之一的信息，均应判定为个人信息。

个人信息举例

个人基本资料	个人姓名、生日、性别、民族、国籍、家庭关系、住址、个人电话号码、电子邮件地址等
个人身份信息	身份证、军官证、护照、驾驶证、工作证、出入证、社保卡、居住证等
个人生物识别信息	个人基因、指纹、声纹、掌纹、耳廓、虹膜、面部识别特征等
网络身份标识信息	个人信息主体账号、IP 地址、个人数字证书等
个人健康生理信息	个人因生病医治等产生的相关记录，如病症、住院志、医嘱单、检验报告、手术及麻醉记录、护理记录、用药记录、药物食物过敏信息、生育信息、以往病史、诊治情况、家族病史、现病史、传染病史等，以及与个人身体健康状况相关的信息，如体重、身高、肺活量等

个人教育工作信息	个人职业、职位、工作单位、学历、学位、教育经历、工作经历、培训记录、成绩单等
个人财产信息	银行账户、鉴别信息(口令)、存款信息（包括资金数量、支付收款记录等）、房产信息、信贷记录、征信信息、交易和消费记录、流水记录等，以及虚拟货币、虚拟交易、游戏类兑换码等虚拟财产信息
个人通信信息	通信记录和内容、短信、彩信、电子邮件，以及描述个人通信的数据（通常称为元数据）等
联系人信息	通讯录、好友列表、群列表、电子邮件地址列表等
个人上网记录	指通过日志储存的个人信息主体操作记录，包括网站浏览记录、软件使用记录、点击记录、收藏列表等
个人常用设备信息	指包括硬件序列号、设备 MAC 地址、软件列表、唯一设备识别码（如 IMEI/Android ID/IDFA/OpenUDID/GUID/SIM 卡 IMSI 信息等）等在内的描述个人常用设备基本情况的信息
个人位置信息	包括行踪轨迹、精准定位信息、住宿信息、经纬度等
其他信息	婚史、宗教信仰、性取向、未公开的违法犯罪记录等

附件五：个人敏感信息

个人敏感信息是指一旦泄露、非法提供或滥用可能危害人身和财产安全，极易导致个人名誉、身心健康受到损害或歧视性待遇等的个人信息。通常情况下，14 岁以下（含） 儿童的个人信息和涉及自然人隐私的信息属于个人敏感信息。可从以下角度判定是否属于个人敏感信息：

泄露：个人信息一旦泄露，将导致个人信息主体及收集、使用个人信息的组织和机构丧失对个人信息的控制能力，造成个人信息扩散范围和用途的不可控。某些个人信息在泄漏后，被以违背个人信息主体意愿的方式直接使用或与其他信息进行关联分析，可能对个人信息主体权益带来重大风险，应判定为个人敏感信息。例如，个人信息主体的身份证复印件被他人用于手机号卡实名登记、银行账户开户办卡等。

非法提供：某些个人信息仅因在个人信息主体授权同意范围外扩散，即可对个人信息主体权益带来重大风险，应判定为个人敏感信息。例如，性取向、存款信息、传染病史等。

滥用：某些个人信息在被超出授权合理界限时使用（如变更处理目的、扩大处理范围等），可能对个人信息主体权益带来重大风险，应判定为个人敏感信息。例如，在未取得个人信息主体授权时，将健康信息用于保险公司营销和确定个体保费高低。

个人敏感信息举例

个人财产信息	银行账户、鉴别信息(口令)、存款信息（包括资金数量、支付收款记录等）、房产信息、信贷记录、征信信息、交易和消费记录、流水记录等，以及虚拟货币、虚拟交易、游戏类兑换码等虚拟财产信息
个人健康生理信息	个人因生病医治等产生的相关记录，如病症、住院志、医嘱单、检验报告、手术及麻醉记录、护理记录、用药记录、药物食物过敏信息、生育信息、以往病史、诊治情况、家族病史、现病史、传染病史等

个人生物识别信息	个人基因、指纹、声纹、掌纹、耳廓、虹膜、面部识别特征等
个人身份信息	身份证、军官证、护照、驾驶证、工作证、社保卡、居住证等
其他信息	性取向、婚史、宗教信仰、未公开的违法犯罪记录、通信记录和内容、通讯录、好友列表、群组列表、行踪轨迹、网页浏览记录、住宿信息、精准定位信息等

您如需了解更多检测内容和技术解决方案，请访问小米开放平台 https://dev.mi.com 咨询【小米客服】或检测评估机构【捷兴信源】。