白牌安全与隐私合规要求

一、目的

为规范第三方供应商合作的流程及管控措施，降低合作中的风险，确保公司信息安全与合规，特制定此管理规范。

二、适用范围

本管理规范适用于 OPPO 互联网服务系统与白牌供应商合作的应用。

注：白牌应用指，由三方负责开发并且负责 App 主要功能的数据处理的，oppo 方不提供或者仅提供帐号登录、支付结算等技术支持，由 oppo 方和三方按照合同约定进行收入分成的应用。

三、常见个人信息分类分级

常见个人信息分类分级标准				
第一类别	**第二类别**	**第三类别**	**第四类别（明细列举）**	**级别**
用户个人数据（定义：用户的基本信息和用户提供给 *oppo* 使用的数据）	**个人一般信息（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。）**	**个人基本资料**	生日、性别、民族、国籍、头像、昵称等	M
		网络身份识别信息	IP 地址、wifi 列表、账号 ID（如 ssoid）等	M
		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、证书&职称等	M
		个人常用设备信息	软件列表（app 下载与安装列表）、指包括硬件序列号（如 IMEI、SN、CPLC）、设备 MAC 地址、唯一设备识别码（如 android ID/IDFA/OPENUDID/GUID、SIM 卡 IMSI 信息等）、OpenID、SSID、MCC、MNC、手机型号、系统版本号等在内的描述个人常用设备基本情况的信息	M
		个人健康生理信息	体重、身高、肺活量等	M
		运动信息	步数、步频、运动时长、运动距离、运动方式、运动心率等	M
		个人通信衍生信息	描述个人通信的数据（通常称为元数据，如通话时长）等	M
		个人金融信息	主要为机构内部信息资产，供内部使用的个人金融信息：	M
			账户开立时间、开户机构、基于账户信息产生的支付标记信息	

		用户自定义信息	主动公开的个人信息，如：用户社区发表帖子与图片、用户社区评论回复内容等	M
		个人位置信息	GPS	M
	个人敏感信息（定义：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）儿童的个人信息和自然人的隐私信息属于个人敏感信息。	**个人基本资料**	个人电话号码、个人姓名、家庭关系、住址（含收货地址）、电子邮箱等	H
		网络身份识别信息	个人信息主体账号（支付宝账号、QQ 号、微信账号）、邮箱地址等	H
			个人信息主体账号有关的密码、口令、口令保护答案、用户个人数字证书、短信验证码等	H
		儿童个人信息	14 岁以下（含）儿童的个人一般信息	H
		个人生物识别信息	个人基因、指纹、声纹、掌纹、耳廓、虹膜、面部特征等	H
		个人身份识别信息	身份证、军官证、护照、驾驶证、户口、工作证、社保卡、居住证等	H
		联系人信息	通讯录、好友列表、群列表、电子邮件地址列表等	H
		用户个人通信信息	通信记录和内容、短信、彩信、电子邮件等	H
		个人位置信息	包括行踪轨迹、精准定位信息、住宿信息等	H
		个人常用设备信息	IMEI（欧盟）	H
		其他产品相关信息	日程、录音、照片、视频、便签、浏览器书签、收藏夹等	H
		用户行为信息	网站浏览记录、软件使用记录、功能使用记录、点击记录、搜索记录、行为日志、搜索关键词、下载记录、收藏列表、语音指令、用户使用某业务的行为记录（如：游戏业务：用户游戏登录时间、最近充值时间、累计充值额度、用户通关记录）	M
		（个人上网记录）		
		用户画像信息	能指明个人的用户行为偏好、年龄、性别、地域等画像与标签信息	M
		其他信息	性生活或性取向、婚史、宗教或哲学信仰、未公开的违法犯罪记录、商业/工会团体资格、种族等	H

四、个人信息全生命周期安全隐私合规要求

个人信息处理活动与产品研发相关，如需上线发布的App、网站、小程序、快应用、H5等涉及个人信息收集、处理、分享的，应在需求阶段进行安全与隐私合规评审（详见附录A），并在上线前至少两周申请安全与隐私合规测试。未经安全与隐私合规评审，未通过安全与隐私合规测试，不得上线。

数据全生命周期	个人信息通用安全与隐私合规要求
收集	**告知同意** 1. App首次运行时，应采取技术措施（如弹窗、提醒勾选、突出链接等）*（禁止默认勾选）*向用户告知个人信息保护政策，并获得明示同意。 2. App应区分基础功能和附加功能，不得强迫用户一揽子授权同意。不得因为用户拒绝提供非必要个人信息，而拒绝用户使用基本功能服务。不得强迫用户同意使用附加功能，不得强迫用户同意非最小必要或者与服务场景无关的个人信息处理行为。 3. 处理个人生物特征信息的，应当对用户进行单独告知，取得用户同意后才可进行处理。 4. 未经用户明示同意，不得通过短信、电话、邮件、应用内通知等方式向用户推送营销信息，且应给与用户便捷且真实的退订/撤回同意/关闭的途径。 5. 未经用户明示同意，不得将用户个人信息用于定向推送、广告精准营销或个性化推荐，且应为用户提供关闭该功能的选项。 6. 在取得用户同意前或者用户明确表示拒绝后，不得收集和处理个人信息。 7. 隐私政策内容发生实质性变更（如数据收集范围、目的变更，获取权限变更等）时，需要再次弹窗告知并要求用户明示同意。 **个人信息保护政策** 8. 个人信息保护政策应披露下述内容，包括但不限于： a) 对个人敏感信息[1]、具体授权内容等应采取加粗、斜体、下划线等足以引起个人信息主体注意的提示； b) 应逐一列出APP各项功能（包括嵌入的第三方代码、插件、SDK、使用Cookie等同类技术等）收集与使用个人信息的目的、方式、范围等，以及存储地域和期限等； c) 需要向第三方提供个人信息的，应当披露涉及数据范围、分享目的、第三方类型或身份等； d) 应向用户说明其享有的数据权利，例如访问、更正、撤回同意、删除、注销账户、隐私投诉等，并说明具体的操作实现路径。 9. 用户进入App主界面后，需在4次（含4次）点击等操作内访问到个人信息保护政策。 **关联启动与自启动**

[1] 个人敏感信息定义请参见第三章。

		10. 关联启动或自启动的情况应当与个人信息保护政策中披露的一致。 11. 在非服务所必需或者无合理场景下，不得自启动或者关联启动其他 App。 **间接获取数据** 12. 从外部机构收集数据的，需注意： a) 收集数据应取得用户同意且仅将数据用于用户授权同意的目的； b) 与第三方数据合作伙伴开展数据合作时，应要求合作方承诺其数据来源合法性并要求合作方提供证明材料，以确认个人信息主体已授权同意转让、共享、公开披露等。如超出原授权范围处理个人信息的，应另行征得用户的明示同意； c) 应通过合同协议等方式，明确双方数据保护责任及义务、数据合作范围及用途等，不得与拒绝履行数据保护义务的合作方开展合作。
传输		1. 外网域名应使用加密协议传输（如 https 等）。 2. 应根据个人信息的安全级别，采用技术手段保证个人信息的安全传输，如安全通道、数据加密等技术措施。
存储		1. 个人信息在客户端应进行加密存储，级别 H 的数据在服务端应进行加密存储。 2. 保存期限以实现服务及管理目的所必须的最短时间为限，不得永久存储，超过期限后应删除或匿名化处理相关信息。 3. 中国大陆、印度、印尼产生的个人数据应在本地存储。
使用	**共享和转让**	1. 未经安全隐私合规评审，禁止共享和转让个人信息（包括对外分享和集团内共享）； 2. 对外共享数据应要求合作方签署数据保护协议/条款/承诺函，明确双方在数据安全方面的责任及义务，并约定共享数据的的内容、用途和使用范围等； 3. 应部署信息防泄露监控工具，监控及报告个人信息的违规外发行为。
数据跨境		在中国大陆、印度、印尼提供产品或服务过程中收集和产生的个人信息，应在本地存储、处理，不得跨境（包括跨境访问）。
删除		1. 对于超出数据保存期限的个人信息，应在产品和服务所涉及的系统中删除或匿名化，使其保持不可被检索和访问； 2. 个人信息主体要求删除个人信息或注销账号时，除法律法规另行规定或与个人信息主体另行约定时，应对个人信息主体的请求予以响应，及时删除相关信息，同时应留存相应删除记录； 3. 在停止提供产品或服务时，应及时删除或匿名化提供产品和服务过程中所收集的个人信息。
销毁		1. 应具备个人信息销毁策略和管理制度，明确销毁对象、流程、方式和要求； 2. 应对个人信息存储介质销毁过程进行监督与控制，对待销毁介质的等级、审批、介质交接、销毁执行等过程进行监督； 3. 销毁过程应保留有关记录，记录至少应包括销毁内容、销毁方式与时间、销毁人签字、监督人签字等内容；第三方存储数据需要删除的，要求第三方出具已删除声明书/承诺书；

	4. 存储个人信息的介质如不再使用，应采用不可恢复的方式（如消磁、焚烧、粉碎等）对介质进行销毁处理；存储个人信息的介质如还需要继续使用，不应只采用删除索引、删除文件系统的方式进行信息销毁，应通过多次覆写等方式安全擦除。

五、权限合规指引

序号	合规场景	子序号	合规要求	详细指引
1	**权限声明**	1.1	提供权限使用说明	(1)内销版本和海外版本采用三合一方案： 隐私通知和权限声明合并为一个声明弹窗。在声明中对应用所需的敏感权限进行说明，以及提供隐私政策和用户协议的链接。 (2)如果业务采用独立的权限声明弹窗界面，需与安全、法务团队评审；

		1.2	权限声明内容	(1)权限声明中对于敏感权限[22]的描述，需要逐一说明应用可能会用到的全部敏感权限及其使用目的，不能使用“等、例如”之类的不完整列举方式。例外情况和补充说明： a)对于非预置应用(即从软件商店等外发渠道下载安装的应用)，权限声明中可只列举和说明首次启动时所需要申请的敏感权限； b)权限声明不能代替权限申请弹窗，同意权限声明不表示应用已获取敏感权限； c)需要逐一声明的敏感权限，原则上与 Manifest 中的敏感权限一一对应； (2)如果需要联网、使用 NFC 或者蓝牙，则需要相应地对联网、NFC、蓝牙权限的使用进行说明。 (3)如果需要使用设备管理器、辅助功能、监听通知栏、悬浮窗权限、后台截屏等特殊敏感操作(非运行时权限)，也需要相应地在隐私声明中进行说明。 (4)对敏感权限描述的粒度，不能只到权限组粒度，而需要对具体敏感行为（基本对应到单个子权限）进行明示，不能用权限组来代替，但可适当合并。例如： a)“发送短信、接收短信”不能以“短信权限”来说明； b)“读取日程、写入或删除日程”不能以“日历权限”来说明； c)“获取手机识别码、获取手机通话状态、拨打电话”，不能以“电话权限”来说明。 d)“读取存储空间、写入存储空间”，可以用“读写存储空间”或“使用存储空间”来说明； (5)声明内容需遵循统一文案格式和措辞，采用软工在各 ColorOS 大版本上的弹窗模板，以及经法务评审。 (6)在隐私政策中应告知用户所接入的第三方 SDK 名称或类型，以及申请的敏感权限、目的等。 Note：第三方应用可能只在权限声明中说明 APP 首次启动时申请的敏感权限，其余的敏感权限放在隐私政策中进行说明。由于 OPPO 的应用基本上都是预置应用，这种方式不满足工信部对预置应用的合规要求，因此 OPPO 应用采用在权限声明里统一声明全部敏感权限的方案。
		1.3	权限声明可退出	声明界面必须提供退出或取消选项，用户不同意时，点击退出或取消选项可退出 APP。

[2] 请参考附录 A《安卓敏感权限清单》

2	**权限弹窗顺序**	2.1	权限弹窗顺序	(1)推荐顺序：(隐私通知+权限声明)->权限申请 (2)APP 首次弹窗的声明中的隐私政策、用户协议链接如需联网，需要单独弹出联网申请(浏览器等已报备的应用除外)，用户同意后再联网访问链接。
3	**预授权**	3.1	新增预授权通过评审	新增预授权必须经安全和法务的评审通过之后向软工申请。使用预授权的规则如下： (1)根据 google 原生的预授权原则进行预授权，如拍照 APP 可申请拍照权限作为预授权，录音机 APP 可申请录音权限作为预授权。 (2)遵从权限最小化原则，预授权限必须是业务能正常使用的最小必要权限，非业务基本功能所需要的权限不能申请预授权。 (3)参考行业实践(对比其他手机厂家同类型 APP 的预授权)。
4	**权限申请时机**	4.1	首次启动时申请	(1)APP 运行所需的最小权限(通常情况下最多是设备标识符权限和存储权限)，可以在首次使用 APP 时弹窗申请。 (2)APP 核心主业务所需要的权限(如地图、生活服务类 APP 所要的位置权限),可以在首次使用 APP 时弹窗申请。
		4.2	实时申请	用户在 APP 中使用到敏感权限相应的子功能时（如浏览器的扫码，对应相机权限），实时弹窗申请。
5	**权限申请**	5.1	按子权限粒度申请	(1)业务所不需要的子权限，不在 Manifest 文件中声明。特殊情况向安全团队备案说明，例如：业务版本 P/Q 共包时，在 P 版本需要申请 READ_PHONE_STATE 权限获取 IMEI，而在 Q 版本不能获取 IMEI 从而也不需要申请 READ_PHONE_STATE 权限，但仍在 Manifest 中有列出。 (2)同一权限组的多个子权限权限可以一次性申请。但如果 APP 只需要权限组下的一个子权限，则只能申请该子权限，不能申请权限组下其他的子权限，例如：当 APP 仅需要使用读取日历权限时，不应申请写入日历权限。
		5.2	同时申请多个权限要求(组合授权)	(1)只在首次使用 APP 时，才能对多个权限申请作合并。在使用 APP 过程中实时申请权限，只能逐个申请。

		5.3	提供开关和不再询问选项	(1)合并多个敏感权限申请时，界面上对每个敏感权限单独提供开关选项或下拉选项。 (2)必须提供“不再询问”选项，两种方式均可：a.总是展示“不再询问”选项；b.默认不展示，但手动关闭任意一个敏感权限时展示。
6	**不给权限不让用**	6.1	首次启动APP时，用户不授权仍可进入APP浏览	APP首次启动时，向用户索取电话、通讯录、位置、短信、麦克风、相机、存储、日历等敏感权限，如果用户拒绝授权后，APP不能退出或关闭，而应仍然能进入应用主界面进行基本的浏览等操作。
		6.2	在APP中使用到需要授权的功能时，用户拒绝授权不退出或关闭APP	APP运行时，向用户申请当前服务场景所需敏感权限，用户拒绝授权后，APP不能退出或关闭。 例如：浏览器中使用扫码功能时向用户申请摄像头权限，用户拒绝后不能退出浏览器。
7	**过度索取权限**	7.1	仅申请APP提供服务所必须的权限	(1)不能以广告、定向推送目的，而专门申请某项敏感权限。如：APP不能仅为了推送基于位置的广告而申请位置权限，且该APP无其他的基于位置的服务。 (2)APP宜对其集成的第三方代码或SDK使用的权限进行审核，保障引入第三方代码或SDK所需使用的权限最小化。如果第三方SDK所需的额外权限，不是APP的服务所必须，则不能申请。 (3)不能以提升用户体验、改进产品功能为由，而专门申请某项权限。
		7.2	权限可解释	APP申请的每一个敏感权限，都能在APP上映射到相应的功能或服务，且在隐私政策中有相应的说明。

8	**频繁申请权限**	8.1	用户拒绝授权后不频繁申请权限	(1)用户明确拒绝权限申请后，不能向用户频繁弹窗申请开启与当前服务场景无关的权限； (2)用户主动触发的权限申请：用户在使用 APP 内相应的业务功能时，如果该功能需要使用到敏感权限则进行权限申请，用户拒绝授权时， a)如果用户没有选择“拒绝并不再询问”选项，则用户再次主动使用该业务功能时，可再次弹窗申请该权限； b)如果用户选择了“拒绝并不再询问”，则用户再次主动使用该业务功能时，不能弹窗申请权限，只能通过文案提示或者提供跳转选项，引导用户到 APP 的“设置”中手动开启权限； (3)非用户主动触发的权限申请：APP 内不是由用户主动触发的功能而申请的敏感权限，如果用户拒绝授权，则在 48 小时内不得再次申请。
		8.2	对敏感权限使用和敏感操作，使用频率符合业务功能需要	(1)位置权限：非地图导航类应用，应用自动申请频率应小于 5 次/每分钟。 (2)设备识别码(IMEI/MAC 地址等)：应用自动申请频率应小于 5 次/每分钟。 (3)敏感权限使用如通讯录、相机、麦克风、通话记录、短信权限，或者其他敏感操作如后台截屏、读写剪贴板等：按需使用，只有在用户主动触发这些权限或敏感操作所对应的业务功能时使用，不能后台自动访问。 (4)第三方 SDK 调用敏感权限的频率也应与 SDK 的功能相匹配，如果第三方 SDK 调用敏感权限频率超过实际需要，应及时通知第三方 SDK 整改或进行替换。 Note：以上数据为已有应用的测试经验值，如 APP 实际超过该频率基线值，需向安全团队进行澄清说明。
9	**权限查看**	9.1	提供权限查询功能	ColorOS 7.0 及以上版本均已支持查看 APP 所有权限； ColorOS 7.0 以下版本不支持查看系统应用的预授权；
10	**权限撤销**	10.1	提供权限撤销功能	ColorOS 7.0 及以上版本均已支持撤销 APP 所有已授予权限； ColorOS 7.0 以下版本不支持撤销系统应用的预授权； 如果部分预授权无法撤销(如撤销之后中能导致系统异常)，则作灰显处理，这类预授权需要向软工申请。

		10.2	撤销后再申请授权要求	参考第 8.1 项。
11	**权限弹窗 UX**	11.1	权限声明 UX	采用软工提供的统一的“应用声明”UX,统一声明的风格。 Note：如业务有特殊原因不采用统一的声明方案，转而采用其他形式的声明方案，则需要经安全、法务进行单独评审。
		11.2	权限申请弹窗 UX	(1)内销版本：采用 OPPO 自研弹窗；海外版本：采用谷歌原生弹窗； (2)权限弹窗需要提供“拒绝并不再询问”选项；
12	**应用升级**	12.1	APP 升级之后，不能变更用户原来的权限授权设置	APP 升级之后，不能变更用户原来的权限授权设置。如果升级后的应用有新增或修改权限，则依照第 4 项“权限申请时机”，在相应时机进行权限申请。

六、SDK 合规要求

序号	要求	内容
1	最小权限获取与信息采集	SDK 应用具备合理的采集个人信息的需求，不采集本业务功能需求以外的个人信息，不申请本业务功能以外的权限。并在合作前提交所需权限与信息采集需求清单，作为安全与隐私合规测试的依据。
2	信息采集需告知用户 SDK 采集个人信息的，应将所采集的个人信息类型及采集使用的目的、范围等告知个人信息主体，具体包括以下情形：	1）功能性 SDK（即 SDK 采集的个人信息由 APP 控制）：SDK 提供者应提供 SDK 采集个人信息类型及采集使用的目的、范围等信息，由 APP 向个人信息主体告知并应征得个人信息主体同意。
3		2）SDK 从 APP 间接获取个人信息：APP 应向个人信息主体告知信息对外提供情况并应征得个人信息主体同意。
4		3）SDK 提供者是直接个人信息控制者（即 SDK 提供者通过 SDK 直接采集个人信息，APP 不能控制收集到的个人信息）：SDK 提供者应提供 SDK 采集个人信息类型及采集使用的目的、范围等信息，并通过 SDK 本身或 APP 向个人信息主体告知并应征得个人信息主体同意。
5		4）SDK 与 APP 同是个人信息控制者（即 SDK 提供者通过 SDK 直接采集个人信息，APP 同时也可以控制收集到的个人信息）：SDK 提供者应提供 SDK 采集个人信息类型及采集使用的目的、范围等信息，SDK 与 APP 各自或共同向个人信息主体告知并应征得个人信息主体同意。
6		5）SDK 采集个人信息类型及采集使用的目的、范围发生变化的，应当更新告知，并重新征得个人信息主体同意。

7	禁止提前采集个人信息	向用户告知个人信息收集使用情况并征得其同意前，SDK 不得采集个人信息。SDK 不得提前向用户申请权限。
8	禁止热更新	尽量采用不使用热更新或热修复技术的三方 SDK，包括 Jar 替换、插件化技术和流行的 Hotfix、Tinker、Robust、Sophix 等三方热更新方案。确需使用，需要向安全团队进行报备经审批后才可以使用。 A、明示自身 SDK 存在热更新机制； B、热更新推送前至少两周向安全团队提供本次更新的完整安装包用于安全和隐私合规测试，测试通过后方可发布热更新； C、针对热更新包提供有效的校验方式； D、热更新包不可使用不受保护的外部存储临时存放； E、具备热更新功能的 SDK 宜保留 App 开发者在不接受热更新推送功能情况下，仍可正常使用 SDK 其他相关功能的权利。
9	开源合规要求	1. 第三方 SDK 提供者的交付物中必须提供开源软件使用声明，声明其 SDK 使用了哪些开源软件，具体信息包括但不限于：软件名称、版本号、许可证等。如没有使用开源软件，亦应明确声明未使用。
10		2. 三方保证不得将其提供的适用 GPL 许可证（或其他类似的著佐权许可证）的代码与我方软件（包括但不限于我方自主研发、委托其他三方研发的软件以及从其他三方处购买的软件）代码作为一个整体组合使用（“使用”指类库引用、修改后的代码或者衍生代码），即不得“传染”我方的软件，从而需要我方将我方的软件代码开源。

附录 A 安卓敏感权限

序号	权限组	子权限	功能描述	可访问的个人数据
1	CALENDAR(日历)	READ_CALENDAR	读取日历	系统日历中的日程安排、备忘、行程等信息
2		WRITE_CALENDAR	编辑日历	
3	CALL_LOG(通话记录)	READ_CALL_LOG	读取通话记录	用户通话记录
4		WRITE_CALL_LOG	编辑通话记录	
5		PROCESS_OUTGOING_CALLS(安卓 Q 删除)	查看正在拨打的号码，并监听、控制或中止通话	用户呼出的电话号码、呼叫状态等信息
6	CAMERA(相机)	CAMERA	使用摄像头	拍照、二维码、条形码、录像、人脸识别、智能识图等
7	CONTACTS(通讯录)	READ_CONTACTS	读取通讯录	用户通讯录(联系人信息)
8		WRITE_CONTACTS	编辑通讯录	
9		GET_ACCOUNTS	从账户服务中获取应用账户列表	账户服务中 APP 账户列表
10	LOCATION(位置)	ACCESS_FINE_LOCATION	获取精准地理位置(基于 GPS 等)	精准地理位置
11		ACCESS_COARSE_LOCATION	获取粗略地理位置(基于基站、IP 地址等)	粗略地理位置
12		ACCESS_BACKGROUND_LOCATION(安卓 Q 新增)	后台运行时访问用户的位置(需要应用先获得访问精准位置或粗略位置权限)	实时地理位置信息、行踪轨迹
13	MICROPHONE(麦克风)	RECORD_AUDIO	使用麦克风录音	录音内容
14	PHONE(电话)	READ_PHONE_STATE	获取设备 IMSI、IMEI 等设备识别码，还可以获取电话通话状态，如来电、通话中、响铃中等	安卓 Q 之前：设备识别码(IMEI、IMSI 等)、通话状态。 安卓 Q：获取通话状态。
15		READ_PHONE_NUMBERS	获取本机手机号码	手机号码
16		CALL_PHONE	拨打电话	实时通话行为

17		ANSWER_PHONE_CALLS	接听电话	
18		ADD_VOICEMAIL	添加语音邮件	语音邮件内容
19		USE_SIP	拨打/接听 SIP 网络电话	实时网络通话行为
20		ACCEPT_HANDOVER	允许 APP 继续进行在其他 APP 中发起的通话	
21	SENSORS(身体传感器)	BODY_SENSORS	获取传感器数据，如心率传感器数据	心率等身体传感器数据
22	SMS(短信)	SEND_SMS	发送短信	实时短信行为
23		RECEIVE_SMS	接收短信	
24		READ_SMS	读取短信、彩信	短信、彩信内容
25		RECEIVE_MMS	接收彩信	接收彩信行为
26		RECEIVE_WAP_PUSH	接收 WAP 推送信息	WAP 推送信息内容
27	STORAGE(存储)	READ_EXTERNAL_STORAGE(安卓 Q 删除)	读取外置存储器	存储的个人文件
28		WRITE_EXTERNAL_STORAGE(安卓 Q 删除)	写入外置存储器	
29		ACCESS_MEDIA_LOCATION	读取媒体文件中的位置信息	照片拍摄地点信息
30		READ_MEDIA_IMAGES(安卓 Q 新增)	读取图片	存储的个人文件
31		READ_MEDIA_VIDEO(安卓 Q 新增)	读取视频	
32		READ_MEDIA_AUDIO(安卓 Q 新增)	读取音频	
33		读取图片（READ_MEDIA_IMAGES）安卓 Q 新增		
34		读取视频（READ_MEDIA_VIDEO）安卓 Q 新增		
35		读取音频（READ_MEDIA_AUDIO）安卓 Q 新增		
36	PHYSICALACTIVITY(健身运	ACTIVITY_RECOGNITION	检测用户动作（例如步行，骑车或坐车）	特定身体活动变化信息，如未移动、步行、

	动，安卓 Q 新增)			跑步、骑车等
37	NFC	近距离通讯操作 (android.permission.NFC)		
38	蓝牙	使用蓝牙 (android.permission.BLUETOOTH)		
39	特殊敏感权限	PACKAGE_USAGE_STATS （读取应用使用情况）	获取其他 APP 的使用统计数据，如使用频率、时长，以及语言设置等使用记录	
40		BIND_DEVICE_ADMIN (设备管理器)	激活使用设备管理器	
41		BIND_ACCESSIBILITY_SERVICE （辅助模式）	使用无障碍功能，通过屏幕取词、模拟用户点击等方式，方便用户操作	
42		BIND_NOTIFICATION_LISTENER_SERVICE (监听通知栏)	监听其他 APP 通知栏显示的内容	
43		SYSTEM_ALERT_WINDOW (悬浮窗)	在其他 APP 上覆盖显示	
44		WRITE_SETTINGS (读写系统设置)	读取或修改系统设置	
45		读取剪贴板		
46		获取应用列表		