TC260-PG-20205A

网络安全标准实践指南

—移动互联网应用程序（App）中的第三方软件开发工具包（SDK）安全指引

（征求意见稿）

全国信息安全标准化技术委员会秘书处

2020 年 9 月

本文档可从以下网址获得：
www.tc260.org.cn/

全国信息安全标准化技术委员会
NATIONAL INFORMATION SECURITY STANDARDIZATION TECHNICAL COMMITTEE

前　言

《网络安全标准实践指南》（以下简称《实践指南》）是全国信息安全标准化技术委员会（以下简称“信安标委”）秘书处组织制定和发布的标准相关技术文件，旨在围绕网络安全法律法规政策、标准、网络安全热点和事件等主题，宣传网络安全相关标准及知识，提供标准化实践指引。

声　明

技术支持单位

本《实践指南》得到中国电子技术标准化研究院、腾讯、360、百度、小米、阿里巴巴、蚂蚁金服、滴滴出行、中国移动、浙江每日互动、华为、字节跳动、京东数科、美团、友盟+、哈啰出行、京东、高德等单位的技术支持。

摘　要

当前，第三方软件开发工具包（SDK）被广泛应用于各类移动互联网应用程序（App）的开发中，由第三方SDK带来的安全问题已经引起多方关注。2020年央视“3.15”晚会曝光了第三方SDK违法违规收集用户个人信息的问题，在社会上引起了强烈反响。

本文件针对当前第三方SDK使用过程中存在的第三方SDK自身安全漏洞、恶意第三方SDK、第三方SDK违法违规收集App用户的个人信息等问题，结合当前移动互联网技术及应用现状，给出了App提供者、第三方SDK提供者针对第三方SDK安全问题的实践指引，旨在减少因第三方SDK造成的App安全与个人信息安全问题。

目　录

1. 适用范围

本指引针对当前第三方 SDK 使用过程中存在的第三方 SDK 自身安全漏洞、恶意第三方 SDK、第三方 SDK 违法违规收集 App 用户的个人信息问题，结合当前移动互联网技术及应用现状，给出了 App 提供者、第三方 SDK 提供者针对第三方 SDK 安全问题的实践指引。

本指引适用于 App 提供者和第三方 SDK 提供者在使用和提供第三方 SDK 时作为参考。App 提供者包括 App 开发者和运营者，第三方 SDK 提供者包括第三方 SDK 开发者和运营者。

SDK 中又嵌入其他 SDK 的，主动嵌入的一方可参考对 App 提供者的措施建议，被嵌入的一方可参考对 SDK 提供者的措施建议。

2. 第三方 SDK 概述

软件开发工具包（Software Development Kit，简称SDK）是指辅助开发某一类软件的相关文档、范例和工具的集合。第三方SDK是指由第三方服务商或开发者提供的实现软件产品某项功能的工具包，通常不包括企业自己开发的仅供自己使用的通用功能模块。

当前，第三方SDK被广泛应用于各类App的开发中。按所提供的功能划分，常见的第三方SDK有框架类、广告类、推送类、统计类、地图类、社交类、支付类、客服类等（详见表1）。按来源划分，可大致分为第三方服务商提供类和开源社区提供类，开源社区提供的第三方SDK又可分为有明确开发主体和无明确开发主体。

表 1 常见第三方 SDK 类型列表

序号	SDK 分类	功能描述
1	框架类	提供开发某一类 App 或跨平台 App 所需的整体框架。

序号	SDK 分类	功能描述
2	广告类	提供广告展示功能，通过使用广告 SDK，App 提供者可以在 App 中展示广告商投放的广告，进而根据用户的点击赚取收益。
3	推送类	提供消息推送功能。
4	统计类	提供收集用户与 App 之间的交互行为的功能。根据用户使用 App 的情况，开发者可以有针对性地改进 App。
5	地图类	提供地图和定位功能。
6	第三方登录类	提供通过其他账号体系（如微博、微信、QQ）等第三方账号登录 App 的功能。
7	社交类	提供社交功能，如消息、分享、排行等功能。
8	支付类	提供移动支付功能。
9	客服类	提供客服对话窗口、客服机器人等客服功能。
10	测试类	提供线上测试功能，如 AB 测试。
11	安全风控类	提供移动业务安全风控功能。
12	Crash 监控类	提供 App 崩溃、App 无响应、卡顿的数据收集与分析。
13	人脸识别类	提供人脸识别、活体检测等功能。
14	语音识别类	提供语音转文字等功能
15	短信验证类	提供短信验证功能。
16	基础功能类	提供 App 的基础功能，如网络访问、图片缓存等。

第三方SDK将实现特定功能的代码进行封装，向App提供者提供简单的调用接口，使App提供者不必关心所需功能的具体代码实现便能使用相关功能，极大地简化了App开发和运营的过程，提高了App开发和运营的效率。但也正因为如此，第三方SDK自身的行为具有较强的隐蔽性，其所造成的安全问题不易被察觉。此外，一款第三方SDK可能会被多款App集成，因此一旦该SDK出现安全问题，就会影响多款App及其用户。

3. 第三方 SDK 安全问题

第三方SDK常见的安全问题可分为以下三类:

3.1 第三方 SDK 自身安全漏洞

第三方 SDK 在开发时聚焦于功能的实现，而忽视了安全性，导致 SDK 本身存在安全漏洞,如常见的 SSL 通信客户端信任任意证书、HTTPS 关闭主机名验证、Webview 忽略 SSL 证书错误等（详见附录 A）。这些漏洞可能被恶意攻击者利用，对大量嵌入该 SDK 的 App 及其终端用户的数据及隐私安全造成严重威胁，例如典型的 ZipperDown 漏洞事件[1]。ZipperDown 漏洞是由于使用第三方 Zip 库解压 Zip 文件的过程中没有对 Zip 内文件名做校验导致，如果文件名中含有“../”文件路径则可以实现目录的上一级跳转，从而实现 App 内任意目录的跳转，进一步可以实现文件覆盖，攻击者便可以对应用资源、代码进行任意篡改、替换，从而实现远程代码劫持等高危操作，危害应用业务场景。

3.2 恶意第三方 SDK

恶意第三方SDK是指嵌入App中的SDK自主实施恶意行为。某些恶意第三方SDK在嵌入App的初期可能并不具有恶意行为，但可后续通过热更新动态加载恶意代码，实施恶意行为（如图1所示），例如典型的“寄生推”事件[2]。在“寄生推”事件中，SDK开发者可以通过云端控制的方式对目标用户下发包含恶意功能的代码包，进行Root提权，静默应用安装等隐秘操作，进而通过恶意广告行为和应用推广

[1] ZipperDown 漏洞，炒作还是一触即发？ https://www.freebuf.com/articles/terminal/172627.html
[2] “寄生推”SDK 云控作恶，300 多款应用不幸躺枪. https://www.freebuf.com/articles/terminal/168984.html

牟取灰色收益，受影响App多达300余款，潜在可影响近两千万用户。

常见恶意第三方SDK的行为分类如表2所示。

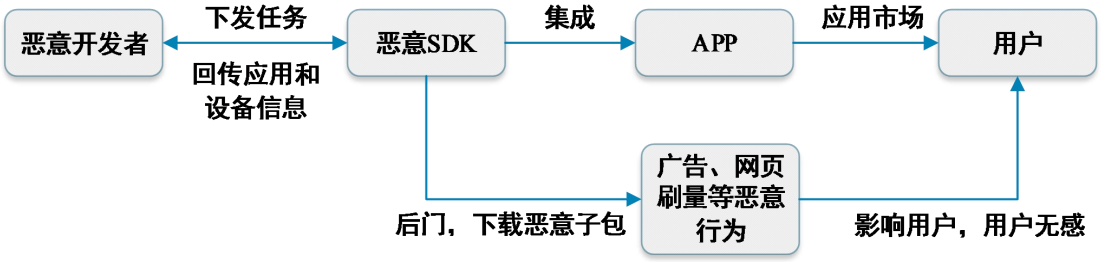

图 1 恶意 SDK 动态更新后隐蔽执行恶意行为

表 2 第三方 SDK 恶意行为分类

序号	行为名称	注释
1	流量劫持	第三方SDK信息拉取、上报和展示目标与App提供者设定的目标不同，恶意劫持App流量，可能产生不良事件。
2	资费消耗	第三方SDK可通过消耗用户网络套餐资费、恶意发送收费短信，订阅收费服务等行为，造成用户的资金损失。
3	隐私窃取	第三方SDK在用户不知情或误导用户的情况下，隐蔽窃取用户的通讯录、短信息等个人敏感信息，隐蔽进行拍照、录音等敏感行为，并发送给恶意开发者。
4	静默下载安装	第三方SDK在后台静默下载、安装其它恶意软件或病毒木马。
5	广告刷量	第三方SDK在用户不知情的情况下，通过后台模拟人工点击广告链接的行为来牟利。
6	恶意广告	第三方SDK向用户推送包含欺诈内容、病毒木马的广告链接。推送过量广告，进而长期占用系统通知栏、屏幕界面，干扰用户正常使用App。
7	勒索	第三方SDK恶意加密用户手机中的文件，干扰用户对手机的正常使用，并以恢复正常使用为由向用户勒索钱财。
8	挖矿	第三方SDK在用户不知情的情况下利用其手机的计算能力来为攻击者获取电子加密货币，对用户设备硬件造成性能损耗。

序号	行为名称	注释
9	远程控制	第三方SDK在手机端启动本地后台服务器，接收远程控制端发来的控制指令，隐蔽进行上述其他恶意行为。

3.3 第三方 SDK 违法违规收集 App 用户的个人信息

第三方SDK可以独立具备收集和使用用户个人信息的能力，例如，一些第三方SDK会读取用户设备的IMEI、Android Id等设备标识符，读取用户设备已安装应用程序列表，读取用户通信录、通话记录、地理位置等敏感信息，并将收集的信息进行处理后，用于人物画像、定向推送、安全风控等业务场景。然而，第三方SDK通常不会向用户告知收集使用个人信息的目的、方式、范围，且在未经用户同意的情况下，私自收集个人信息，或私自向其他应用或服务器发送、共享用户个人信息。由于第三方SDK通常无法独立展示前台页面，无法直接向用户告知收集使用个人信息的目的、方式、范围，其告知行为通常需要借助宿主App来实现。而宿主App未进行告知的原因主要包括两方面：一方面是第三方SDK提供者未向App提供者告知或未完整告知自身所收集的个人信息，进而App提供者也无法向用户进行明确告知；另一方面是第三方SDK提供者告知了自身所收集的个人信息，但App提供者未在此基础上向用户进行明确告知。

4. 措施建议

建议App提供者、第三方SDK提供者针对第三方SDK安全问题进行排查，评估相关安全风险，并参考以下措施建议，优化安全防护策略。

4.1 对 App 提供者

a) 应遵循合法、正当、必要的原则选择使用第三方SDK。

b) 在集成第三方SDK前宜对第三方SDK进行安全性评估，包括：

1) 来源安全性评估，包括但不限于：SDK提供者的基本信息；SDK提供者的沟通反馈渠道；SDK隐私政策链接地址；SDK提供者的安全能力；SDK的基本功能；SDK的版本号；SDK的安全性评估报告等。

2) 代码安全性评估，包括但不限于：是否存在已知的恶意代码；是否存在已知的安全漏洞；是否申请敏感权限[3]；是否嵌入了其他第三方SDK等。

3) 行为安全性评估，包括但不限于：调用的敏感权限、目的和频率；收集的个人信息类型、目的和频率；个人信息回传服务器域名、IP地址、所在地域；是否存在热更新行为及热更新是否可主动关闭；传输数据是否加密；是否存在单独收集用户个人信息的界面；是否存在后台自启动和关联启动后收集个人信息的行为等。

c) 宜使用提供者基本信息明确、沟通反馈渠道有效的第三方SDK。

d) 对于使用的具有热更新功能的第三方SDK，宜对第三方SDK的热更新内容进行内容校验、动态检测和安全评估，对于非官方的热更新内容进行阻断，对于发现问题的热更新内容应及时停用。

[3] 本文件所指的敏感权限，是指可访问用户个人信息（如短信、通信录、设备唯一标识符等）和可调用敏感操作能力（如摄像头、麦克风、精确地理位置等）的系统权限。

e) 宜对集成后的第三方SDK进行持续动态监测或定期进行安全评估。对于已经发现的第三方SDK安全漏洞，及时修复，或者采用其它替代方案，并从第三方SDK官方渠道及时更新最新版本SDK。对于已经发现存在恶意行为的第三方SDK，及时停止使用。

f) 通过接口调用第三方SDK功能的，宜对接口增加鉴权机制。

g) 宜向用户告知所接入的第三方SDK的名称或类型，第三方SDK收集的个人信息类型、目的和方式，申请的敏感权限、申请目的等，并征得用户同意。若第三方SDK需向用户单独告知收集使用个人信息的行为，App宜为其中无单独页面的第三方SDK提供向用户告知的便捷渠道。

注：例如可通过在App隐私政策中嵌入第三方SDK隐私政策链接的方式进行告知。

h) 宜与第三方SDK提供者签订合作协议或进一步完善与第三方SDK提供者的合作协议，明确第三方SDK收集的个人信息类型、申请的敏感权限、个人信息的收集目的、保存期限、超期处理方式等，明确双方在个人信息保护方面分别应采取的措施、承担的责任和义务等。当双方合作存在重大变更时，应重新达成合作协议。

i) 停用某第三方SDK后，宜及时从App中移除该第三方SDK的代码和调用该第三方SDK的代码，存在通过本App共享或收集个

人信息的，应敦促第三方SDK提供者按照合作协议约定，删除从本App共享或收集的个人信息或做匿名化处理。

4.2 对第三方 SDK 提供者

a) 收集使用个人信息和申请敏感权限应遵循合理、最小、必要原则。

b) 对功能独立的模块，宜进行拆分或提供单独的开启关闭选项，允许App提供者按需进行选择使用或开启关闭，不应强制捆绑无关功能并以此为由申请无关权限或收集无关的个人信息。

c) 宜通过代码审计、代码混淆等方式，增强自身安全性。在发布上线前，宜进行安全评估，形成安全评估报告，评估内容包括但不限于：完整性校验、恶意代码检测、安全漏洞检测、权限申请和调用频率检测、收集个人信息类型和频率检测、后台自启动和关联启动并收集个人信息的行为检测。

d) 通过接口调用提供自身功能的第三方SDK，宜对接口增加鉴权机制，并对不同App调用接口的上下文环境进行隔离。

e) 宜为不同的App提供者设置逻辑独立的数据存储区域，不同App之间的数据宜相互独立。

f) 数据传输宜使用HTTPS安全信道、双向证书校验、证书绑定等安全机制，避免因中间人攻击导致传输数据泄露或被篡改。传输用户个人敏感信息的，宜对个人敏感信息单独进行加密。

g) 采用热更新技术的第三方SDK，宜建立完善的热更新安全保障机制，包括但不限于：

1) 宜向App提供者明示自身SDK存在热更新机制；

2) 宜在热更新推送前至少5个工作日向App提供者说明本次热更新包更新的时间节点、热更新的具体内容、更新后可能造成的影响、热更新包的有效校验方式等；如果热更新内容涉及个人信息收集使用的目的、方式和范围的变更，安全性变更或重大的功能变更，宜进一步通过邮件、短信等逐一触达的方式告知App提供者；

3) 宜提供单独控制热更新功能开启关闭的选项，说明关闭热更新功能带来的影响，并保留App提供者在不接受热更新功能的情况下仍可正常使用SDK其他功能的权利。

h) 宜向App提供者告知第三方SDK的相关信息，告知的信息应完整、准确、及时，不存在故意隐瞒、欺骗等行为。告知内容包括但不限于：SDK提供者的基本信息、沟通反馈渠道、安全能力；SDK的基本功能、版本号、隐私政策链接地址、安全性评估报告；申请的敏感权限和申请目的；收集的个人信息类型和收集目的[4]；个人信息回传服务器所在地域；热更新机制及其开启关闭方式；是否存在单独收集用户个人信息的界面；嵌入的其他可收集个人信息的第三方SDK；是否向其他应用或服务器发送、共享收集的用户个人信息等。

[4] 对于必须要申请的敏感权限或必须要收集的个人信息，宜进一步说明其必要性。

i) 作为个人信息共同控制者或独立控制者收集使用用户个人信息的第三方SDK，宜单独向用户告知收集使用个人信息的行为并征得用户同意。（告知同意的文案可参考附录B）。

j) 在保障安全的前提下，宜优先在本地的App私有存储空间内存储和处理个人信息。在本地存储和处理个人敏感信息，宜单独进行加密。

k) 宜采用可变更的标识符取代不可变更的设备唯一标识符

l) 宜建立响应个人信息主体请求和投诉等机制，并在接入App前及时告知App提供者相应的请求和投诉渠道，以供个人信息主体查询、使用。

m) 宜建立“Opt-out”退出机制，当个人信息主体不希望使用第三方SDK提供的服务时，个人信息主体可通过“Opt-out”机制行使退出权利[5]。宜在官网或个人信息保护政策中透出“Opt-out”的链接，以便个人信息主体行使权利。

n) 宜完善与App提供者的合作协议，明确第三方SDK收集的个人信息类型、申请的敏感权限、个人信息的使用目的、保存期限、超期处理方式等，明确双方在个人信息保护方面分别应采取的措施、承担的责任和义务等。当双方合作存在重大变更时，应重新达成合作协议。

[5] 例如，友盟+，终端设备 Opt-out。
https://outdip.umeng.com/opt_out.html?spm=a213m0.13887608.0.0.3cb275ef0jDEVu

o) 当某App停止接入后，若存在从该App共享或收集个人信息的，应按照合作协议约定，删除从该App共享或收集的个人信息或做匿名化处理。

附录 A 常见第三方 SDK 安全漏洞

表 3 常见第三方 SDK 安全漏洞

类型	名称
源文件安全	Java 代码未混淆风险
	私有函数调用风险
	AES 弱加密漏洞
	RSA 算法不安全使用漏洞
	随机数不安全使用
	敏感函数调用风险
内部数据交互安全	低保护级别的自定义权限
	PengdingIntent 不安全使用
	隐式意图调用
	动态注册广播
	FFmpeg 文件读取
	Intent Scheme URLs 攻击
	Provider 文件目录遍历
	Fragment 注入
	Webview 未移除隐藏接口
	Webview 明文保存密码
	Activity 绑定 browserable 与自定义协议
	存在剪切板读或写操作漏洞检测
通信数据传输安全	SSL 通信服务端检测信任任意证书
	SSL 通信客户端检测信任任意证书
	HTTPS 关闭主机名验证
	Webview 存在本地 Java 接口
	Webview 忽略 SSL 证书错误
	开放 socket 端口
	Webview 启用访问文件数据

本地数据存储安全	getdir 读写权限配置错误
	全局文件读写权限配置错误
	配置文件读写权限配置错误
	AES/DES 硬编码密钥
	打开或创建数据库文件权限配置错误
防御检测	DEX 文件动态加载
	外部加载 so 文件漏洞
	未使用编译器堆栈保护技术
	未使用地址空间随机化技术
	unzip 解压缩（ZipperDown）
	动态链接库中包含执行命令函数
	libupnp 栈溢出漏洞
	Webview 组件远程代码执行（调用 getClassLoader）
	保存明文数字证书风险
	篡改/二次打包风险
	资源文件泄露风险
	so 文件破解风险

附录 B 第三方 SDK 告知同意

第三方 SDK 提供者在采集使用用户个人信息前，应向用户明示其收集使用个人信息的目的、方式与范围、调用权限的类型与目的，并征得用户同意。如涉及信息回传或分享等行为，也应当告知用户。

考虑到第三方 SDK 的使用场景及产品形态不同、第三方 SDK 与 App 之间的法律关系不同，宜结合产品形式和具体场景设计告知同意的形式，使用户理解此场景中的数据控制者以及个人信息处理规则：

（一）若 SDK 提供者独立决定收集个人信息的目的和类型，SDK 为数据控制者，或者 SDK 存在用户可见的界面，在产品形态允许的情况下，SDK 宜自行通过弹窗或者其他友好界面的方式向用户展示应告知内容，至少通过产品界面展示 SDK 服务提供者身份。

注：如电商网站的支付 SDK，点击支付 SDK 服务商的图标后会跳转到 SDK 对应的页面上进行登录以及支付，在此场景下支付 SDK 独立收集并处理支付相关的个人信息，支付 SDK 宜在用户注册或使用服务时告知用户，展示应告知内容，并征得用户的同意。

（二）若 SDK 提供者作为数据处理者，按照 App 提供者的要求处理个人信息，或 SDK 无用户可见的界面，App 提供者宜在 App 启用相关 SDK 前告知用户 SDK 收集个人信息的相关内容。SDK 提供者宜在其与 App 提供者的合同、公开的开发者文档等公示 SDK 收集的个人信息、调用的权限以及目的等信息（可以是独立的《XX SDK 隐私政策》文档）。此情形下，告知形式可参考如下文案：

1、SDK 隐私政策正文：

____ SDK 是____（SDK 提供者）开发的，被集成于____ App 产品或服务中，用于为用户提供____服务的产品。在此场景中，____ App 提供者作为数据控制者决定用户数据的处理目的、方式，____（SDK 提供者）在为用户提供____服务过程中作为数据处理者，接受____ App 提供者委托并根据____ App 提供者指示处理用户数据。为了说明 ____ SDK 会如何收集、使用和存储您的个人信息及您享有哪些权利，我们将通过本隐私政策向您阐述相关事宜。请您仔细阅读《____ SDK 隐私政策》并确定了解我们对您个人信息的处理规则。如您不同意协议中的任何条款，请您向____ App 提供者提出主张停止使用____ SDK 服务或者通过____（联系方式）与____（SDK 提供者）联系。

(以下为正文内容，参考《信息安全技术 个人信息安全规范》通用产品隐私政策模板即可)

2、SDK 开发者官网公开的开发者文档/公开声明：

为保证贵司合法使用____ SDK 服务，建议在 App 的隐私政策中增加以下条款，或以其他方式获得用户同意。

“我们的产品或服务可能包括第三方的产品或服务，也可能收集并使用您的个人信息。例如，我们为实现____服务集成____ SDK，____（第三方 SDK 提供者）将作为数据处理者，按照本公司的指示收集处理您的数据，____（第三方 SDK 提供者）将按照《____ SDK 隐私政策》（附链接）所述收集、处理、保护您的个人信息。”

3、SDK 与 App 提供者的合同示例：

（1）当 SDK 提供者独立决定收集个人信息的目的和类型，SDK 为数据控制者时:

如 App 提供者使用____ SDK 服务，____（第三方 SDK 提供者）将收集提供服务所必须的个人信息，因此，____（第三方 SDK 提供者）应保证事先获得终端用户同意以使____ SDK 有权收集并使用其个人信息提供相应服务。如果终端用户未作出同意，则____ SDK 不应进行数据收集和处理行为，App 提供者也不应继续使用____ SDK 服务。

双方同意遵守适用的终端用户数据收集、使用、披露及保护相关的法律法规、政策和行业标准，并确保符合该等法律法规、政策及行业标准的规定。

____ SDK 对用户个人信息的具体收集使用行为包括：（具体说明收集使用的个人信息类型、方式和范围等）。____ SDK 承诺遵守适用的隐私法律法规规范规定，并按照 APP 提供者的指示进行数据处理....

（2）当 SDK 提供者作为数据处理者时

如 App 提供者使用____ SDK 服务，____（第三方 SDK 提供者）将收集提供服务所必须的个人信息，因此，____（第三方 SDK 提供者）强烈建议 App 提供者仔细阅读____（第三方 SDK 提供者）公示的声明，将关键条款包含进 App 提供者产品面向终端用户的隐私政策中，并保证链接准确有效，即 App 提供者应保证事先获得终端用户同意以使____ SDK 有权收集并使用其个人信息提供相应服务。如

果终端用户未作出同意，则 App 提供者不应继续使用____ SDK 服务。前述关键条款____（第三方 SDK 提供者）已起草模板供您参考。您可根据实际业务场景进行修订或完善，但应确保完整性与真实性。如因 App 提供者未事先获得终端用户同意以使____ SDK 有权收集并使用其个人信息提供____服务而引起的相关责任由 App 提供者承担。____ SDK 负责确保提供内容的真实性和准确性。

App 提供者同意遵守适用的终端用户数据收集、使用、披露及保护相关的法律法规、政策和行业标准，并确保符合该等法律法规、政策及行业标准的规定使用____ SDK 服务。作为____ SDK 服务的使用者，App 提供者必须制定、发布您的隐私政策并获得终端用户同意，且该政策应不低于____ SDK 的隐私保护标准。但是，____（第三方 SDK 提供者）不控制 App 提供者如何使用属于或关于 App 提供者终端用户的数据，也不应为此负责。

____ SDK 对用户个人信息的具体收集使用行为包括：（具体说明收集使用的个人信息类型、方式和范围等）。____ SDK 承诺遵守适用的隐私法律法规规范规定，并按照 APP 提供者的指示进行数据处理....