软件开发工具包（SDK）合规治理研究报告

（2026 年）

中国互联网协会知识产权工作委员会

上海倍孜网络技术有限公司

2026年7月

版权声明

前　言

随着我国数字经济的蓬勃发展，软件开发工具包（SDK）产业市场规模不断增长，SDK 应用范围不断扩大。SDK 通过封装复杂的功能和流程，使得开发者能够轻松地将各种服务和特性集成到自身的产品中，极大地提高了开发效率、降低了开发成本，促进了移动应用程序（App）和小程序的快速创新。然而，随着 SDK 的广泛应用，其安全性和合规性问题逐渐成为公众和监管机构关注的焦点。

本报告由中国信息通信研究院编制。首先，报告概述了 SDK 产业的市场背景和发展现状，并对 SDK 相关的法律法规、规范性文件、标准进行了梳理。其次，报告详细识别和评估了 SDK 在个人信息保护、数据安全、不正当竞争、消费者权益保护、广告合规、刑事合规等方面的风险。再次，报告分别梳理了 SDK 提供者、集成者和第三方行业机构探索出的 SDK 合规治理实践经验和解决方案。最后，报告提出要以“技管结合”“多方协同”为准则，共同推动 SDK 行业的安全合规发展。

本报告希望能够为 SDK 行业的所有参与者提供参考，帮助相关方在享受 SDK 带来的便利和效率的同时，也能够开展有效管理、降低风险。期待与业界同仁共同努力，为构建一个更加安全、合规、可持续的 SDK 行业环境做出贡献，报告不足之处欢迎批评指正。

目 录

图 目 录

表 目 录

一、SDK 产业发展及合规治理

（一）数字经济强势增长，SDK 产业发展稳步推进

我国数字经济的发展正以前所未有的速度推进，成为经济变革的重要驱动力。2024 年，我国数字经济规模已达到 59.2 万亿元，同比名义增长 9.69%，占 GDP 比重达到 43.8%，较上年提升 1 个百分点，呈现出稳步增长趋势。[1] 2025 年数字经济核心产业增加值占国内生产总值的比重达到 10.5%以上，核心产业销售收入同比增长 9.4%。[2] 我国数字经济规模及其占 GDP 比重的提升展现出数字经济强劲的增长势头和广阔的发展前景。在全球经济数字化转型、国际格局深刻演变、增长动能转换、全球发展面临诸多不确定挑战的背景下，数字经济展现出强大的韧性与活力，[3] 为我国经济社会发展贡献新动能。

移动互联网作为我国数字经济的重要支柱，其灵活性、便捷性和创新性为我国数字经济的发展提供了强大的动力和广阔的空间。我国移动互联网目前已覆盖线上娱乐、生活消费、教育求职、旅游出行、电商购物、金融理财等众多领域，具备广泛的用户基础。截至 2025 年 12 月，我国移动互联网月活跃用户规模已达 12.76 亿，全网用户月人均单日使用时长及次数分别 7.96 小时和 112.9 次，同比增长 6%和 2.1%。[4] 移动互联网流量也在实现快速增长，2025 年移动互联网接入

[1] 数据来源：中国信通院《中国数字经济发展研究报告（2025 年）》
[2] 数据来源：国家数据局《数字中国发展报告（2025 年）》
[3] 参见中国信通院《全球数字经济发展研究报告--数智驱动与秩序重构（2025 年）》
[4] 数据来源：QuestMobile《2025 中国移动互联网年度大报告》

总流量达 3958 亿 GB，比上年增长 17.3%，全年移动互联网月户均流量（DOU）达 20.7GB/户·月，比上年增长 14.1%。[5]

移动互联网月活用户和接入流量规模的增加一定程度上得益于不断涌现的创新性移动应用程序（App），同时移动互联网的普及使用也促进了对 App 的开发和使用，创造了新的经济增长点。与此同时，小程序在中国市场也已经形成了庞大的用户基础和交易规模。截止 2026 年 3 月，小程序整体月活用户规模已达 10.21 亿，[6]在多个行业中发挥着越来越重要的作用。

随着 App 和小程序市场的快速扩张，以及用户需求的不断提高，App 和小程序开发效率便亟待提升。软件工具开发包（SDK）作为一款集合了二进制文件、API、文档、范例和工具等用于协助开发者进行软件开发的工具包开始进入市场。一方面，SDK 能够避免开发者重复编写创新性较低但又耗时耗力的程式化代码，也能在不了解具体代码细节的情况下快速将某特定功能集成到待开发产品中，进而能够更加专注于对创新性代码的研发和对商业模式的优化，提升开发效率并降低开发成本。另一方面，SDK 能够解决 App 或小程序在不同设备之间的兼容性问题，简化了硬件适配工作，确保所有用户都能无障碍使用相关产品，提升应用在各市场的普及率和可用性。由此可见，SDK 在 App 和小程序的开发和运营中发挥着关键作用。

目前，SDK 在我国已经具备较大的市场规模，主流 App 中基本都集成有 SDK。据统计，国内一款 App 集成的 SDK 数目平均可达 20

[5] 数据来源：国家数据局《数字中国发展报告（2025 年）》
[6] 数据来源：QuestMobile《2026 全景生态流量春季报告》

个以上。目前，市面上主流 App 中集成 SDK 类型主要包括第三方登录社交类、电话号码一键登录类、消息推送类、在线支付类、广告服务类、地图位置类、统计分析类、安全风控类、开发框架类、Crash 监控类、人工智能应用类（包含人脸识别类、语音识别类、AR 技术类等）、基础功能类等，应用场景极为广泛，如表 1 所示。

表 1 10 款主流 App 集成 SDK 类型及数量

	APP 名称	APP 类别	集成 SDK 情况
1	抖音（v31.6.0）	视频播放	消息推送类（7 款）、基础功能类（5 款）、第三方登录社交类（3 款）、在线支付类（3 款）、电话号码一键登录类（3 款）、身份验证类（2 款）、地图位置类（1 款）、统计分析类（1 款）、人工智能应用类（1 款）、广告服务类（1 款），**共 27 款**
2	爱奇艺（v15.9.0）	视频播放	第三方登录社交类（8 款）、电话号码一键登录类（8 款）、消息推送类（4 款）、在线支付类（3 款）、广告服务类（4 款）、基础功能类（4 款）、人工智能应用类（2 款）、统计分析类（2 款）、地图位置类（1 款）、开发框架类（1 款）、安全风控类（1 款），**共 38 款**
3	淘宝（v10.40.11）	电商购物	消息推送类（4 款）、在线支付类（2 款）、地图位置类（1 款）、第三方登录社交类（1 款）、电话号码一键登录类（1 款）、安全风控类（1 款）、统计分析类（1 款），**共 11 款**
4	京东（v13.2.9）	电商购物	第三方登录社交类（6 款）、消息推送类（5 款）、电话号码一键登录类（5 款）、地图位置类（3 款）、身份验证类（2 款）、在线支付类（1 款）、广告服务类（1 款）、基础功能类（1 款）、开发框架类（1 款），**共 25 款**
5	小红书（v13.2.9）	综合	基础功能类（11 款）、消息推送类（9 款）、第三方登录社交类（5 款）、电话号码一键登录类（4

		社交	款）、地图位置类（3 款）、在线支付类（2 款）、开发框架类（2 款）、人工智能应用类（2 款）、统计分析类（1 款）、安全风控类（1 款）、广告服务类（1 款）、身份验证类（1 款），**共 42 款**
6	微博（v14.9.3）	综合社交	基础功能类（10 款）、消息推送类（8 款）、第三方登录社交类（8 款）、电话号码一键登录类（6 款）、人工智能应用类（6 款）、在线支付类（4 款）、身份验证类（1 款）、安全风控类（2 款）、开发框架类（1 款）、广告服务类（1 款），**共 47 款**
7	夸克（v7.3.0.650）	实用工具	第三方登录社交类（5 款）、广告服务类（5 款）、基础功能类（5 款）、消息推送类（4 款）、电话号码一键登录类（4 款）、开发框架类（2 款）、安全风控类（2 款）、地图位置类（1 款）、人工智能应用类（1 款）、统计分析类（1 款）、Crash 监控类（1 款），**共 26 款**
8	QQ 浏览器（v15.5.2.2042）	实用工具	基础功能类（9 款）、消息推送类（5 款）、在线支付类（2 款），**共 16 款**
9	美团（v12.25.204）	便捷服务	消息推送类（8 款）、在线支付类（4 款）、电话号码一键登录类（3 款）、第三方登录社交类（2 款）、基础功能类（3 款）、身份验证类（2 款）、地图位置类（1 款），**共 23 款**
10	百度地图（v20.7.30.1423）	地图导航	第三方登录社交类（6 款）、消息推送类（6 款）、在线支付类（3 款）、广告服务类（3 款）、统计分析类（1 款）、基础功能类（1 款），**共 20 款**

来源：公开资料整理

（二）SDK 合规治理引关注，有关规则不断完善

随着 SDK 产业持续发展，SDK 的合规治理也引起广泛关注。在 2018 年，一款名为“寄生推”的推送 SDK 通过云端控制方式向用户分发了含有恶意功能的代码包，影响了 300 多款应用，潜在影响了近

2000 万用户。在 2020 和 2023 年，央视“3.15”晚会两次曝光了 SDK 违法违规收集用户个人信息的问题，在社会上引起了广泛关注。而且值得注意的是，SDK 一旦出现安全合规问题，不仅会对其自身产生影响，还会使得集成相关 SDK 的 App 产生安全合规问题，造成广泛的影响，因而需要加强对 SDK 的合规治理。而 SDK 合规治理需要完善、明确的规则，以提供更加全面、明晰的合规依据。目前，SDK 合规治理规则主要可以分为法律法规、规范性文件、标准三个层面。

1.法律法规层面

现行法律法规中没有针对 SDK 的直接规定，更多是通过不同部门法对 SDK 可能引发的不同类型的安全合规风险进行调整。

根据当前实践，SDK 具有个人信息处理者、数据处理者等多重身份，最容易引发的是个人信息安全、数据安全方面的风险，所以包括《个人信息保护法》《数据安全法》《网络安全法》等与个人信息、数据安全相关法律法规均能够对 SDK 进行调整。在个人信息保护的部门规章立法进程中，《移动互联网应用程序个人信息保护管理暂行规定（征求意见稿）》较早地、专门地对 SDK 的个人信息保护义务作出了规定。随后，《互联网应用程序个人信息收集使用规定（征求意见稿）》在此基础上进一步细化并确立了 App 开发运营者与 SDK 运营者的双重主体责任，构建了更为清晰的责任框架。目前，这两部重要的规范均处于征求意见稿阶段。

此外，SDK 的相关行为还可能引发不正当竞争、侵害消费者权益、造成刑事犯罪等安全合规风险，进而受到相应法律法规的调整。

2.规范性文件层面

除了法律法规，近年来，工业和信息化部、国家网信办等相关监管部门针对 SDK 安全合规风险，制定了一系列规范性文件，以协助开展 SDK 合规治理，主要包括：

2019 年 11 月，国家网信办、工业和信息化部、公安部、国家市场监管总局根据于同年 1 月发布的《关于开展 App 违法违规收集使用个人信息专项治理的公告》，为有关主体判断 App 是否存在违法违规收集使用个人信息的行为提供参考和指引，共同制定并发布《App 违法违规收集使用个人信息行为认定方法》(以下简称“《认定方法》”)。该文件是首个提及 App 中嵌入的第三方代码、插件（包括 SDK）的规范性文件，但其监管对象仍是 App 运营者，监管重点仍是 App 收集使用个人信息的行为。该文件要求 App 向用户披露其内嵌 SDK 收集使用个人信息的目的、方式、范围等，以及 App 向其内嵌 SDK 提供收集到的个人信息时应取得用户同意。

2020 年 7 月，工业和信息化部发布《关于开展纵深推进 App 侵害用户权益专项整治行动的通知》（以下简称“164 号文”）。该文件首次明确将“软件工具开发包（SDK）提供者”单独作为侵害用户权益的治理对象，不再将其作为 App 服务提供者的附带监管对象，并对 SDK 单独提出合规要求。164 号文重点聚焦 SDK 违规处理个人信息的问题，对 SDK 违规收集个人信息、超范围收集个人信息、违规使用（尤其是未经同意对外提供或共享）个人信息以及强制用户使用定向推送功能等内容进行规范。

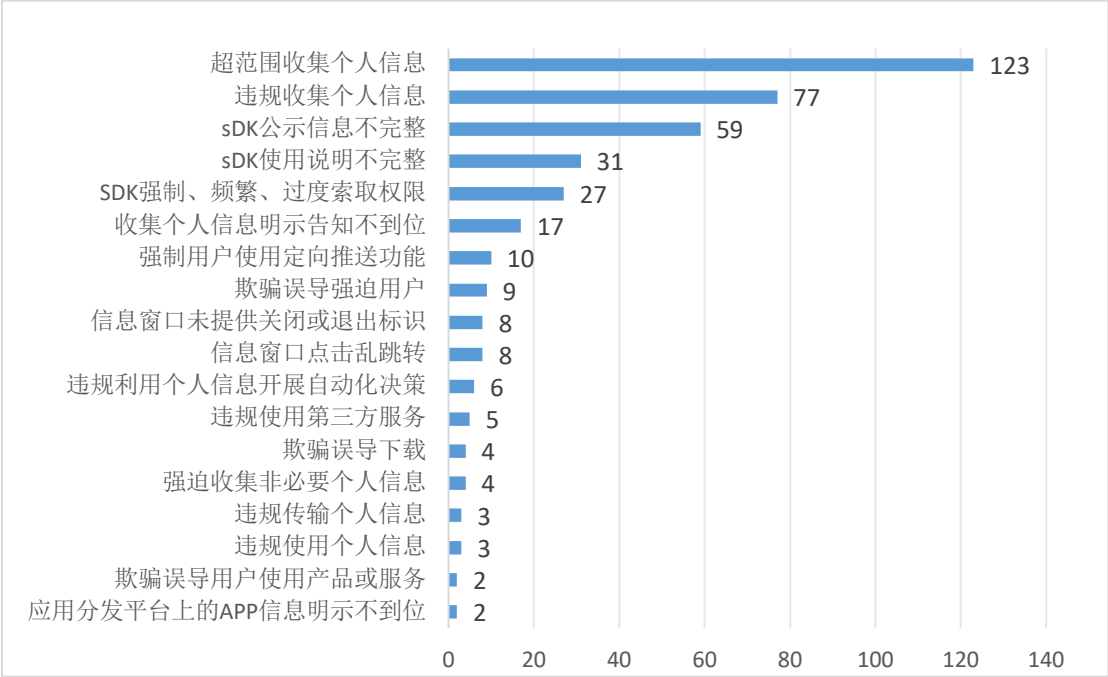
2021 年 11 月，工业和信息化部发布《关于开展信息通信服务感知提升行动的通知》（以下简称“292 号文”）。该文件对内嵌 SDK 及相关 App 开发者均提出要求，但对二者的要求仍然较为独立。对于 App 开发者，292 号文在此前披露要求的基础上进一步提出了建立“已收集个人信息清单”和“与第三方共享个人信息清单”的要求，并且需要在“双清单”列明内嵌 SDK 所收集和被共享个人信息的基本情况，便于用户进行查看。对于内嵌 SDK，292 号文要求其在并非用户正在使用的 App 功能所必须情况下禁止自启动或关联启动，同时要求 App 开发者和内嵌 SDK 均应允许用户能够自主选择是否开启关联启动，这是此前的规范性文件中未曾提及的内容，旨在更进一步提升 SDK 及 App 的个人信息保护能力。

2023 年 2 月，工业和信息化部发布《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》（以下简称“26 号文”）。该文件相较于此前的相关规范性文件，涉及 SDK 的内容篇幅显著增加，并且特别强调了 App 开发运营者与 SDK 服务提供者之间的协同合作，明确双方可能存在共担责任的情况。对于 App 开发运营者，要求其加强 SDK 使用管理，除了此前就有规定的 SDK 相关情况披露义务，使用前还需对 SDK 进行个人信息保护能力评估，并通过合同明晰双方权利义务。对于 SDK 服务提供者，除了要求其建立信息公示机制、优化功能配置，还突出强调了要加强与 App 开发运营者之间的服务协同，通过明确易懂的方式主动向 App 开发运营者提供合规使

用指南，使其能正确合理使用 SDK，并且当 SDK 的个人信息处理规则变更或发现风险时，也应当及时向 App 开发运营者告知。

由此可见，相较于法律法规，有关部门制定的规范性文件更加聚焦对 App 以及与其紧密相关的 SDK 的规范。从规范对象来看，规范性文件由开始主要通过 App 开发运营者对内嵌的 SDK 作出规范，到后来将 SDK 提供者明确作为规范对象进行直接规制。从合规治理涉及的风险类别来看，大部分规范性文件主要聚焦 SDK 个人信息合规治理问题，对于 SDK 可能引发的其他类型安全合规风险涉及较少。从合规治理的具体要求来看，规范性文件从对 App 开发运营者和 SDK 提供者分别赋予相应、独立的合规治理义务，转变为鼓励实现相互协同、共同合规。

此外，工业和信息化部及各地方通管局对 App、SDK 的通报是检测相关监管治理专项工作和相应规范性文件要求落实情况的最主要手段。2022 年 2 月 18 日，工业和信息化部首次将 SDK 作为与 App 并列的项目进行通报，在通报 2022 年第一批侵害用户权益的 App 的同时，提到了 13 款内嵌第三方软件开发工具包（SDK）存在违规收集用户设备信息的行为。从此之后，涉及 SDK 安全合规的执法案例在工业和信息化部和地方管局的执法实践中屡见不鲜。截至 2026 年 7 月，工业和信息化部共有 32 次通报涉及 SDK 产品，对 173 款 SDK 进行了通报，通报事项共 398 项。被通报 SDK 所涉及的主要问题包括超范围收集个人信息、违规收集个人信息、SDK 使用说明不完整、收集个人信息明示告知不到位等，具体情况如图 1 所示。



来源：公开资料整理

图 1 工业和信息化部通报 SDK 所涉问题及频次

3.标准层面

在 SDK 合规治理的标准制定层面，为配合和支撑工业和信息化部、国家网信办等相关部委的 SDK 合规治理的规范要求落地，有关国家标准、团体标准的编制工作逐步开展。

2020 年 11 月，TC260-PG-20205A《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）安全指引》发布。《SDK 安全指引》首次梳理了 SDK 安全合规的常见问题类型，包括 SDK 自身安全漏洞、SDK 恶意行为、SDK 收集使用个人信息三类，并针对常见问题分别向 App 提供者和 SDK 提供者提出了可行的安全措施。之后，在 2022 年和 2023 年，国家标准 GB/T 41391-2022《信息安全技术 移动互联网应用程序（App）收集个人信息要求》和 GB/T 42884-2023《信息安全技术 移动互联网应用程序（App）生命

周期安全管理指南》又针对 App 提供者（运营者）提出嵌入第三方 SDK 时应当采取相应的安全管理措施，以减少 App 受到内嵌 SDK 可能带来的由个人信息合规风险、安全漏洞和恶意行为风险引发的负面影响。其中，《App 收集个人信息要求》提出了限制嵌入 SDK 数量、对 SDK 进行评估、明确 SDK 个人信息处理规则和双方责任、向用户告知 SDK 有关情况、及时删除停止使用的 SDK 代码等要求。《App 生命周期安全管理指南》则是从 App 需求分析、开发设计、测试验证、上架发布、安装运行、更新维护、终止运营共七个阶段，对 App 提供者提出对 SDK 相应的安全管理措施，通过层层监测保护避免相关安全合规风险的发生。在前述标准起草发布和 SDK 合规治理行业实践深化的基础上，国家标准 GB/T 43435-2023《信息安全技术 移动互联网应用程序（App）软件开发工具包（SDK）安全要求》已于 2023 年 11 月 27 日发布，并于 2024 年 6 月 1 日正式实施。作为 SDK 合规治理的最新国家标准，《SDK 安全要求》是相关内容的集大成者。其对 SDK 安全风险的分类基本沿用了此前《SDK 安全指引》的类型划分，仅将收集个人信息安全风险扩展至处理个人信息安全风险，并从 SDK 设计、开发、发布、运营、终止运营全生命周期和 SDK 个人信息收集、存储、使用和加工、传输、提供、公开、删除等处理活动的两个层面进一步细化了对 SDK 运营者的安全要求。《SDK 安全要求》中针对 SDK 运营者提出的合规治理要求与此前的《App 收集个人信息要求》《App 生命周期安全管理指南》中针对 App 提供者提出的合

规治理要求相对应，并且对各类 SDK 安全合规风险均有所回应，由此 SDK 合规治理问题在国家标准层面已形成较为全面完善的规则。

由电信终端产业协会编制第一份 SDK 团体标准 T/TAF 057-2020《移动智能终端应用软件 SDK 安全技术要求》于 2020 年 4 月发布。该标准最早给出了 SDK 相关安全要求，涉及安全集成、权限申请使用、代码安全、行为安全、传输安全、日志安全、存储安全和个人信息收集使用等方面，为后续 SDK 合规治理标准编制提供了参考基础。其中，代码安全要求和行为安全要求从一定程度上可以降低前述提到的 SDK 自身安全漏洞和 SDK 恶意行为所引发的安全风险，其他方面的安全要求则更偏向于防范 SDK 处理个人信息安全风险。2022 年发布的 T/TAF 123-2022《软件开发包（SDK）个人信息处理规范》则在《移动智能终端应用软件 SDK 安全技术要求》的基础上梳理整合并细化，针对 SDK 个人信息处理的场景，规定了 SDK 提供者在个人信息处理各环节的基本要求。此外，相较于其他标准，该标准还特别强调了保障及时响应用户权利的要求。中国互联网协会则于 2021 年 11 月发布了团体标准《移动互联网应用程序 SDK 安全规范》（征求意见稿），该项目于 2023 年 11 月正式实施，且标准正式名称改为 TISC0017-2022《移动互联网应用程序 SDK 安全技术要求及测试方法》。该标准主要聚焦于 SDK 自身安全漏洞，对 SDK 提供者提出基本安全要求、数据存储安全要求、数据交互安全要求、重要组件安全要求、代码及资源安全文件要求，同时针对每一方面要求提出相应的评测规范，为 SDK 提供者开展合规治理提供参考。由此可见，团体

标准和国家标准在 SDK 可能涉及的安全合规风险上具有一致性，但不同的团体标准可能会因为参编单位不同各有侧重，更具有针对性。

相较于监管部门发布的规范性文件，标准文件更加聚焦于 SDK 合规治理问题，有专门规范 SDK 的标准文件，不再是将其与 App 进行共同规范。并且，标准文件系统梳理了 SDK 相关的合规治理问题，并且提出的应对措施也更加具体细致。

综上所述，目前 SDK 合规治理的有关规则正不断完善，且已经初步形成较为完整的体系。从规则内容来看，现有规则以个人信息保护、数据安全为核心，对不同类型的 SDK 安全合规风险均有所涉及和规范，并且既有宏观层面的规定又有微观细致的规定。从规范对象来看，现有规则不仅对 SDK 提供者均提出合规治理要求，还对 App 提供者也提出相应的合规治理要求，期待两类主体能够为 SDK 合规治理共同努力。

二、SDK 安全合规风险

SDK 虽能显著提升应用开发的效率和便捷性，但它们也可能违反现行法律规范，带来诸多安全合规风险，相关主体进而需要承担相应的法律后果。具体而言，SDK 可能引发以下安全合规风险：

（一）SDK 个人信息保护风险引重视

SDK 提供者[7] 作为个人信息处理者在处理个人信息过程中存在个人信息保护风险，从而侵害个人信息主体的个人信息权益，并且有

[7] 前述法律法规、规范性文件、标准化文件中对提供 SDK 服务主体的名称存在细微差别，本报告后文将统称“SDK 提供者”，包括 SDK 开发者、所有者、管理者、运营者等。

关风险可能发生在个人信息处理的全部环节，包括收集、使用、存储、传输、提供、删除等处理环节。因而，SDK 个人信息保护风险也引起了监管部门和企业的重点关注。

1.收集环节

（1）未在收集个人信息前向用户公开 SDK 个人信息处理规则，明示 SDK 处理个人信息的目的、方式和范围等。该行为违反了《个人信息保护法》第七条、第十七条。具体情形可能包括：

• SDK 官网未公示或未完整公示相关 SDK 的个人信息处理规则，SDK 未向 App 等集成 SDK 的产品告知其自身的个人信息处理规则，或者 SDK 履行了告知义务但 App 等集成 SDK 的产品未向用户说明，导致用户无法获悉 SDK 处理其个人信息情况。

• 当产品集成的 SDK 又集成了其他 SDK 时，未展示全部层级 SDK 的个人信息处理规则。

• 未以显著方式、清晰易懂的语言公示 SDK 个人信息处理规则，导致用户难以阅读、难以理解。App 等集成 SDK 的产品未集中展示 SDK 个人信息处理规则，加大用户了解内嵌 SDK 个人信息处理规则的难度。

（2）SDK 未经用户同意收集个人信息。该行为违反了《个人信息保护法》第十三条、第十四条。具体情形可能包括：

• SDK 在用户同意之前，私自收集用户个人信息，或者通过隐蔽、静默地开启有关系统权限、自启动或关联启动等方式收集用户个人信息，如隐蔽收集用户通讯录、短信等敏感个人信息，隐蔽开启拍

照、录音权限收集用户人脸、声音等敏感个人信息，隐蔽监视并获取剪切板中的敏感个人信息。

• SDK 在用户明确表示不同意之后，仍继续收集用户个人信息，或者为了获取用户同意，频繁向用户发起申请，干扰用户的正常使用。

• SDK 实际收集的用户个人信息，或者开启的用于收集个人信息的系统权限，与用户授权的范围不一致。

• SDK 开始在用户授权范围内收集用户个人信息，但事后通过热更新等方式静默改变系统权限、私自收集未经用户同意的个人信息。

• SDK 欺骗误导用户同意收集个人信息或者打开相应收集个人信息权限，或者向用户故意隐瞒收集个人信息的真实意图。

（3）SDK 未提供撤回同意的便捷途径。该行为违反了《个人信息保护法》第十五条。具体表现为，SDK 未在官网或者要求 App 等集成 SDK 的产品提供撤回同意的途径，从而导致用户一旦同意 SDK 处理其个人信息便难以撤回，这实际上变相侵害了用户的同意权，导致其无法随时作出最符合自身真实意图的选择。

（4）SDK 超范围收集个人信息。该行为违反了《个人信息保护法》第六条。具体情形可能包括：

• SDK 收集大量非其自身提供服务所必要的个人信息类型，如在仅需收集一般个人信息的场景收集了大量敏感个人信息。

• SDK 收集超出其提供服务所需精度的个人信息，如在仅需收集模糊位置信息的场景下却收集精确位置信息，在仅需收集位置信息的场景下却收集行踪轨迹等。

• SDK 频繁调用权限和收集个人信息，且调用和收集的次数、频率远超提供服务所需的次数、频率，特别是在静默状态下或在后台运行时调用权限和收集个人信息。

• SDK 一揽子过度收集个人信息，而未根据不同应用场景，明确 SDK 相关功能模块和对应的个人信息收集范围，并提供功能模块及个人信息收集的配置选项。

2.使用环节

（1）SDK 违规使用用户个人信息。该行为实际上侵害了用户的知情同意权，违反了《个人信息保护法》第十三条、第十四条。具体表现为，SDK 超出其声明的个人信息处理规则，将用户个人信息用于其提供服务之外的目的，即超出用户的授权范围使用其个人信息，侵害了用户的同意权。

（2）SDK 强制用户使用定向推送功能。该行为违反了《个人信息保护法》第二十四条。具体以广告类 SDK 为例，为了实现广告精准的个性化推荐，需要使用用户个人信息并根据用户的偏好和特征分析形成用户画像，用于提升广告推荐效果和转化率，但是部分用户对于将搜索记录、浏览记录、使用习惯等个人信息用于形成精准的消费偏好、消费水平等用户画像信息实际上存在排斥心理，SDK 不得剥夺有关用户拒绝的权利。

3.存储环节

SDK 未采取相应措施保障个人信息存储安全。该行为违反了《个人信息保护法》第五章的相关规定。具体表现为，SDK 未采取安全的

方式在移动终端存储用户个人信息，尤其是针对用户敏感个人信息未进行单独加密存储或者完整性校验，可能导致用户个人信息被 SDK 集成者[8]和 SDK 提供者之外的第三方获取。

4.传输环节

SDK 未采取相应措施保障个人信息安全传输。该行为同样违反了《个人信息保护法》第五章的相关规定。具体情形可能包括：

• SDK 在通过网络传输个人信息的过程中未使用 HTTPS 协议等安全传输协议，而是使用不安全的网络协议传输个人信息，导致被传输的个人信息遭遇拦截或恶意篡改。

• SDK 在使用本地服务器的技术架构和方案时，未确认本地服务器与远程服务器通信安全。

• SDK 在传输过程中未对个人信息采取加密处理等安全技术措施，尤其是对于敏感个人数据未采取区别于一般个人信息的安全措施。

5.提供环节

SDK 未经用户同意对外提供个人信息。该行为违反了《个人信息保护法》第十三条、第十四条。具体情形可能包括：

• SDK 向第三方提供个人信息时，未简洁、清晰列出向第三方提供个人信息的种类、使用目的、使用场景和提供方式等，导致用户无法在充分知情的情况下作出同意。

• SDK 在用户未作出同意或者明确拒绝同意的情况下，仍然私

[8] 前述法律法规、规范性文件、标准化文件中对集成并使用了 SDK 的主体采用了不同名称，本报告后文将统称“SDK 集成者”，包括 App 开发者、运营者，小程序开发者、运营者等一切在自身产品中集成嵌入了 SDK 的主体。

自向第三方提供收集到的用户个人信息。

• SDK 在用户主动提出要求，向第三方提供个人信息时，未对用户授权情况进行核查并留存核查日志，导致向第三方提供的个人信息存在种类、方式上的错误。

6.删除环节

SDK 未按要求删除个人信息。该行为违反了《个人信息保护法》第二十一条、第四十七条。具体情形可能包括：

• SDK 在集成者停止接入 SDK 或在 SDK 停止运营后，未及时对从 App 等集成 SDK 的产品获取的用户个人信息进行删除，或者在删除确实存在困难时进行匿名化处理，可能会导致个人信息泄露，侵害终端用户的个人信息权益。

• SDK 未向 SDK 集成者提供个人信息删除途径，使得 SDK 集成者及其用户均能通过该途径删除或者请求 SDK 删除相关个人信息，SDK 在接到请求后应及时进行删除。

• SDK 停止运营后，未主动删除其此前收集到的所有个人信息。

（二）SDK 数据安全、不正当竞争、消费者权益保护、广告违法不容忽视

1.数据安全风险

SDK 除了作为个人信息处理者可能在处理个人信息时侵犯有关权利人的个人信息权益，作为数据处理者还有可能因未能采取相应的数据安全保护措施，履行相应的安全保护义务，进而违反《数据安全法》的相关规定。具体可能情形包括：

• SDK 可能因其自身未对源文件安全、内部数据交互安全、通信数据传输安全、本地数据存储安全、防御渐层等方面的 SDK 潜在自身安全漏洞进行监测，从而导致相关数据存在被泄露至除集成 SDK 的 App 外的第三方主体。

• SDK 可能因其与 App 等集成 SDK 的产品间使用某种接口形式不同，且未对不同产品的上下文进行环境隔离，导致跨应用的数据泄漏或者造成其完整性被破坏。

2.不正当竞争风险

（1）SDK 恶意劫持 App 流量构成不正当竞争

SDK 恶意劫持 App 流量，可能违反《反不正当竞争法》第十二条第二款第一项，即“未经其他经营者同意，在其合法提供的网络产品或者服务中，插入链接、强制进行目标跳转。”

首先，流量在网络空间中是稀缺资源，具有较高价值，具有竞争利益，而流量劫持行为对竞争利益进行了抢夺，妨碍、破坏其他经营者合法提供的网络产品或者服务正常运行的行为本身就具有可责性，扰乱了正常的竞争秩序。其次，SDK 恶意劫持 App 流量显然符合“强制进行目标跳转”的行为模式，同时又具有主观上抢夺交易机会的恶意。最后，流量劫持不仅是对受影响网络实体的直接经济损害，剥夺了其正当的交易机会，还侵犯了用户的自由选择权，妨碍用户进行公平交易。此外，如果这种不当行为被视为合理并演变为行业内的常规做法，将导致整个行业陷入一种不正当的流量竞争和用户权益频繁受侵的负面循环，最终削弱了社会的整体福祉。因此，必须采取措施，

防范和打击流量劫持行为，以保护网络主体的合法权益和维护用户的利益，促进健康的网络环境和行业秩序。因此，该行为具有不正当竞争风险。

（2）SDK 广告刷量构成不正当竞争

SDK 广告刷量是指，SDK 在用户不知情的情况下，在后台模拟人工点击广告链接进行牟利。该行为可能违反《反不正当竞争法》第十二条第二款第四项，即“经营者不得利用技术手段，通过影响用户选择或者其他方式，实施其他妨碍、破坏其他经营者合法提供的网络产品或者服务正常运行的行为”。

首先，提供有偿刷量服务，提供虚高或虚假数据，不正当地利用他人已经取得的市场地位和商誉，为自己谋取商业机会和利益，违背了诚实信用原则和商业道德。其次，利用用户设备在其不知情的情况下，对广告的进行虚假刷量，干扰其他经营者的决策，影响其他经营者的利益。再次，针对有竞争关系的产品或服务，实施对特定互联网产品或服务的虚假刷量行为，欺骗和误导用户和消费者，侵害了用户和消费者的知情权和选择权等合法权益。同时，虚假刷量行为损害了社会公共利益，扰乱了正常市场秩序和良性竞争关系。因此，该行为具有不正当竞争风险。

3.消费者权益保护风险

（1）SDK 未保护消费者个人信息

SDK 侵害用户个人信息权益的同时，可能也会构成对用户消费者权益的侵害。随着对个人信息保护的日益重视，除了《个人信息保

护法》，《消费者权益保护法》第二十九条、《消费者权益保护法实施条例》第二十三条也规定，经营者具有保护消费者个人信息的义务，包括收集使用消费者个人信息需经消费者同意等内容。换言之，经营者若未保护消费者个人信息，则构成对消费者权益的侵害。例如，2023 年央视“3·15”晚会曝光了一款 App 的非法破解版本，该破解版 App 被植入了 3 款 SDK。并且，这些 SDK 一旦被激活，便能在用户毫不知情的情况下悄无声息地收集其手机上的敏感个人信息，如唯一设备标识符。通过这些个人信息，即便用户更换了手机或电话号码，破解版应用也能够重新定位并持续追踪用户，从而形成精准用户画像。这使得不法分子能够针对性地向用户投放广告，进而通过这种窃取消费者个人信息的方式进行流量变现，侵害了消费者的相关权益。

（2）SDK 恶意广告侵害消费者人身财产安全

SDK 恶意广告是指，SDK 推送含有虚假信息、欺诈信息等有害、违法内容的广告诱导用户点击。该行为可能会违反《消费者权益保护法》第七条所规定的消费者安全保障权，通过可能引起用户兴趣的文字、图片、视频等方式误导、引诱用户点击广告链接，进入可能含有违法贷款、赌博等内容的网站，导致用户人身财产安全遭受损害，严重侵犯了消费者的安全保障权。

4.广告违法风险

除了可能造成侵害消费者权益的风险，SDK 作为广告发布者也可能因推送明知含有虚假信息或者违法内容的广告，违反《广告法》的规定并承担相应的行政责任。

同时，《互联网广告管理办法》中也对广告发布者施加了显著标明“广告”义务，确保一键关闭义务，建立健全和实施互联网广告业务的承接登记、审核、档案管理制度，配合开展广告监测和互联网广告行业调查、核对下一级链接中与前端广告相关的广告内容等义务。若 SDK 存在未履行上述义务的情况，也需承担相应责任。实践中，部分 SDK 可能会存在推送过量广告并且难以关闭或关闭后反复推送，从而干扰影响用户对产品服务的正常使用，这有可能构成对一键关闭义务的违反。

（三）SDK 刑事犯罪风险后果严重

1.计算机犯罪

由于 SDK 一般是被集成到 App 中使用，具有一定隐蔽性，因而很容易被利用于开展计算机犯罪。例如，浙江法院曾判决一起有关广告 SDK 的刑事案件，该案中的行为人通过预置广告 SDK，在用户不知情的情况下自动联网运行并收集用户设备信息等个人信息，以向用户推送商业广告并获取广告费收入。行为人还通过该 SDK 静默下载安装“一键达 apk”，该 apk 能够模拟用户操作，自动关注目标公众号。最终，行为人的相关行为被认定为使得用户手机依据行为人的意愿进行活动，构成采用技术手段非法控制他人计算机信息系统，应当依法承担相应的刑事责任。

具体而言，SDK 可能构成计算机犯罪的常见具体情形包括：SDK 在后台静默下载、安装恶意软件或木马病毒；SDK 向用户展示含有木马病毒的广告链接，用户点击后导致病毒被植入用户收集设备；SDK

在用户手机设备中启动本地服务器，以接收远程控制指令，从而秘密执行其他恶意操作；SDK 在用户不知情的情况下控制其手机设备，并利用其算力挖掘电子加密货币，对手机设备硬件造成性能损耗。根据《刑法》第二百八十五、二百八十六条的规定，上述情形可能构成非法控制计算机信息系统罪或者破坏计算机信息系统罪。首先，上述情形无论是通过恶意软件、木马病毒，还是任何其他方式，只要达到能够控制操纵目标手机设备的目的，均构成非法控制计算机信息系统罪。其次，若在控制的基础上，同时危害到用户手机设备的安全，造成其相关功能不能正常运行的严重后果，则能够进一步构成破坏计算机信息系统罪。

2.财产犯罪

SDK 还可能通过恶意行为侵犯公民的财产安全，违反《刑法》分则第五章规定的侵犯财产罪。实践中，SDK 可能侵害用户财产安全的方式包括：SDK 未经用户同意消耗用户的网络流量；SDK 向用户发送未授权的付费短信；SDK 在用户不知情的情况下订阅付费服务；SDK 恶意加密用户手机中的文件，妨碍用户正常使用手机，并以此为要挟，向用户勒索赎金以恢复手机功能等。

3.侵犯公民个人信息罪

《刑法》第二百五十三条之一规定了侵犯公民个人信息罪。SDK 若涉及非法获取、出售或提供个人信息，达到司法解释所规定的情节严重的程度而可能构成犯罪时，SDK 提供者或相关责任人除了承担民事责任、行政责任，还需承担相应的刑事责任。

三、SDK 合规治理实践

（一）SDK 提供者、集成者采取合规举措保护个人信息和开发集成安全

1.保护用户个人信息安全

个人信息保护风险是 SDK 所面临最常见的合规风险，并且现有规则对于 SDK 个人信息保护的要求最为全面具体，因而目前 SDK 提供者和 SDK 集成者针对用户个人信息保护问题采取了一系列具体、可操作的合规举措。

（1）SDK 提供者在官网展示 SDK 隐私政策及相关基本信息

SDK 提供者一般会在官网上提供自身的隐私政策，明示处理个人信息的相关情况，并阐明自身数据安全保护能力。部分 SDK 提供者还在隐私政策中会明确区分 SDK 所提供的基础功能和拓展功能，并披露所收集的个人信息以及所开启的设备权限是基础功能的必选类型还是拓展功能的可选类型。同时，若 SDK 中还集成了其他 SDK 或者有向第三方提供个人信息的情况，SDK 官网还会展示合作方清单及相关合作方隐私政策。此外，SDK 提供者还会在其官网上清晰、详细地展示每一款 SDK 的名称、开发者、版本号、主要功能、使用说明、更新时间、适用产品等基本信息。

（2）SDK 提供者在官网为集成者提供合规指引

为了帮助 SDK 集成者在开发集成过程中安全合规使用 SDK，SDK 提供者一般会在官网通过设置“合规专区”或者在“开发者支持”页向 SDK 集成者提供 SDK 合规指南。合规指南的内容包括但不限

于：对现行法律法规及政策文件的解读；SDK 集成者在使用 SDK 时应当重点关注的收集、使用、存储个人信息等全流程处理环节的具体合规点；SDK 集成者隐私政策、第三方共享清单形式上合规的要求；针对不同类别 SDK 制定的具体合规配置说明，明确不同类别 SDK 的可调用权限及可调用时机、SDK 基础功能和拓展功能可采集的个人信息字段，同时提供功能配置方案及示例代码；对 SDK 提供者和 SDK 集成者处理用户个人信息的权责界分；简单的合规视频教程辅助 SDK 集成者理解指南内容；等等。

（3）SDK 提供者根据服务功能划分独立模块

为了尊重 SDK 集成者的选择权和控制权，同时确保其能够遵循最小必要原则进而保障用户个人信息被合规收集使用，部分 SDK 提供者为 SDK 的部分独立功能模块提供了单独的启用和禁用选项。SDK 集成者可以根据自己的需求选择所需的特定功能模块配置相应代码，不会被强制捆绑无关功能，不会被自动开启无关权限，不会被收集无关个人信息。此外，SDK 集成者还可以通过代码直接指定所需收集的个人信息字段，以实现对数据收集的最小化和业务需求的灵活性之间的平衡。

（4）SDK 提供者在官网提供终端设备 Opt-Out 渠道

为了保障终端用户自身的个人信息权益，SDK 提供者在官网提供了便捷的终端设备 Opt-Out 渠道以满足用户随时撤回同意并退出的权利，用户便不再需要通过 SDK 集成者退出个人信息处理，而是能够直接向处理相关个人信息的 SDK 提供者提出请求，避免了因 SDK

集成者未提供退出渠道或者响应效率低下导致个人信息主体权利难以得到及时保护。

（5）SDK 提供者要求集成者开展合规自查并进行合规评估审查

为了进一步保障 SDK 安全合规使用，明晰与 SDK 集成者之间的责任划分，避免承担相关法律风险，部分 SDK 提供者会要求 SDK 集成者开展合规自查，并提供自查指引，以确保 SDK 集成者明确知悉产品开发过程中应当注意的合规注意点。具体而言，SDK 提供者会要求 SDK 集成者从以下方面出发开展合规自查：SDK 集成者应确保在集成了相关 SDK 的产品通过《隐私政策》向用户披露 SDK 的名称和提供者，逐一告知用户 SDK 收集个人信息的目的、方式和范围并附上 SDK 的《隐私政策》；SDK 集成者应当在其 App 等产品首次运行时通过明显方式提示终端用户阅读《隐私政策》，并在确保取得终端用户的合法授权后再初始化 SDK 以收集处理用户个人信息，部分 SDK 提供者还会要求有关 SDK 集成者在下载集成 SDK 前勾选同意《SDK 下载合规指南》；SDK 集成者通过 SDK 收集的个人信息类型和开启的权限种类是否为所提供服务所必需的；等等。

要求 SDK 集成者开展合规自查的同时，部分 SDK 提供者也会同时开展合规评估审查，为 SDK 安全合规使用设置双保险。在与 SDK 集成者合作前，SDK 提供者会通过 SDK 集成者提供的隐私政策、服务协议等对其进行形式审查，判断 SDK 集成者告知和授权同意机制的合规性，以评估合作风险。在合作开展后，SDK 提供者会进一步对 SDK 集成者进行跟踪，审查其是否披露所集成 SDK 的相关信息，同

时会根据 SDK 内部规定对 SDK 集成者开展个人信息保护影响评估，以便根据风险等级采取相应的措施。

（6）SDK 集成者使用合规技术检测平台辅助日常监测评估 SDK 合规性

部分 SDK 集成者为保证自身开发产品的个人信息保护合规性，会配合使用自身开发或者由第三方开发的合规技术检测平台，对 App 及其所集成的 SDK 进行日常监测。这类平台会根据现行法律法规和规范性文件所关注的合规点，基于代码特征学习匹配算法和大数据分析能力，对相关产品进行自动化检测，从一定程度上减轻了人工审核的负担，并且相较于纯粹的人工审核方式更具有及时性。其目前能够识别的合规点包括违规收集个人信息、超范围收集个人信息、违规使用个人信息、强制用户使用定向推送功能、强制频繁过度索取权限、频繁自启动和关联启动、账号注销难等监管机构主要关注的个人信息保护合规点。

2.规范 SDK 开发、集成安全

除了个人信息保护风险，SDK 还可能因存在安全漏洞和恶意行为而产生数据安全、不正当竞争等一系列安全合规风险。针对潜在的安全漏洞和恶意行为，SDK 提供者一般会在 SDK 开发阶段和集成阶段采取相应措施保障其安全合规性。

（1）开发阶段

SDK 提供者首先会制定一套保证产品开发安全性和高效性的制度体系，包括但不限于研究开发组织管理制度、研发费用核算与管理

办法、产研人员管理制度、安全测试流程等，以规范的制度体系。

在产品设计阶段，SDK 提供者会先分析梳理产品可能会涉及的数据类型，并结合业务要求开展安全风险评估，确保 SDK 仅提供与其声明功能相符合的功能，并通过完整性校验、加密等方式增强 SDK 的数据存储传输安全。在产品测试阶段，SDK 提供者需按照事先制定的内部流程，对架构设计、数据缓存设计、响应时间、线程安全策略等方面开展测试，若发现 SDK 存在安全问题需要通知相关部门及时处置，测试由业务侧和技术侧进行双重监督。在产品运维阶段，SDK 提供者运维团队会开展日常内部监测，在发现潜在或者突发的网络与信息安全事件或者其他可能对产品或者用户造成侵害的安全事件时，按照事先制定的应急预案进行处理，保障 SDK 安全合规运行。部分 SDK 提供者还针对广告违法问题，开发了素材审核功能，保障 SDK 上发布广告的合法合规，助力数字营销行业健康发展。

（2）集成阶段

为了确保 SDK 集成使用的安全合规，一些 SDK 提供者还实施了严格的集成管理规范，包括：确保 SDK 产品符合行业标准，保障 SDK 产品能够与各 SDK 集成者安全兼容；部署集成安全策略，防止恶意代码植入和数据泄露；建立审核机制，对业务逻辑、安全漏洞、越权行为等进行检查，并向 SDK 集成者提供 SDK 安全能力证明，持续保障 SDK 的安全性、合规性及其功能的完善；设立多分发渠道，提供全面的 SDK 集成文档与相应的技术支持，帮助 SDK 集成者高效安全地使用 SDK，从而提高部署、应用质量；等等。

同时，SDK 集成者在集成 SDK 前也会针对 SDK 的合规治理情况开展调研评估，积极履行安全管理义务，避免集成存在严重安全合规风险的 SDK，侵害终端用户的权益。

（二）第三方行业机构助力企业开展 SDK 合规治理

除了企业自身的合规实践和监管部门的督促整改，具有一定行业影响力的中国信通院等部分第三方组织也在 SDK 合规治理中采取了有关举措助力 SDK 安全合规发展，具体包括提供技术检测服务、组织签署行业自律公约、搭建管理服务平台、开展研究活动等。

1.提供技术检测服务

中国信通院于 2021 年 6 月发起“SDK 安全专项行动”，旨在通过其“大数据应用与安全创新实验室”所提供的标准化评估方案和实验环境，对 SDK 产品开展持续的技术检验和评估。最终，约有百款 SDK 产品通过检测并获得了安全评估证书，涉及广告聚合、数据分析、安全风险控制、地图导航等多个领域。该行动得到了业界的广泛认可，为行业的安全、健康和有序发展提供了有力支持。

聚焦到移动互联网广告领域，中国信通院还曾与中国广告协会开展合作，共同推进移动互联网广告第三方自动化工具（包括程序、脚本、接口、SDK 等多种形式）管理工作，开展“移动互联网广告第三方自动化工具”安全测评，从接入规则、代码安全、数据安全等多维度进行全面评估。多家知名互联网企业以及广告监测企业的 20 余款 SDK 参与了该项测评工作。

除中国信通院外，中国金融认证中心、公安部安全与警用电子产

品质量检测中心、中国软件评测中心等第三方独立检测机构也根据相应标准针对 SDK 产品开展第三方技术检测，并颁发认证证书。该举措不仅能够帮助 SDK 提供者提高业务的安全合规性，还能筛选出行业内的领先产品，逐步汇聚行业共识，形成行业最佳实践标准。

2.组织签署行业自律公约

2022 年 5 月，中国信通院以“数据安全共同体计划”为契机，启动了“绿色 SDK 产业生态共建行动”，旨在促成“安全高效开发、规范透明集成、合理充分利用”的产业格局。该行动集结多家 SDK 提供商的力量，共同签署《绿色 SDK 产业生态倡议书》，以此激励企业主动承担起自身的责任，共同促进产业的健康发展。

3.搭建管理服务平台

2022 年 9 月，中国信通院主导建立了“全国 SDK 管理服务平台”，该平台旨在为 SDK 提供者和 SDK 集成者为提供 SDK 政策标准发布、产品信息公示、监管问题处置、用户使用反馈、SDK 个人信息保护技术检测等服务提供一系列服务，通过上述服务促进 SDK 行业的健康和合规发展。

4.开展相关研究活动

一方面，有关组织机构会撰写 SDK 相关研究报告。中国信通院联合深圳市腾讯计算机系统有限公司、北京市环球律师事务相继发布《软件开发包（SDK）安全与合规白皮书》（2019）、《软件开发包（SDK）安全与合规报告》（2020）、《软件开发包（SDK）安全研究报告》（2021）对 SDK 可能产生的安全合规问题进行梳理，并结

合最新的行业实践提出合规管理建议和安全措施建议。国家计算机网络应急技术处理协调中心（CNCERT）与中国网络空间安全协会也于 2021 年 12 月发布了《App 违法违规收集使用个人信息监测分析报告》，指出 SDK 收集个人信息行为的普遍存在，并提出个人信息处理活动需要严格规范。

另一方面，有关组织机构会举办行业研讨会。中国信通院联合深圳市和讯华谷信息技术有限公司、中国互联网协会数据安全与治理工作委员会于2023年7月举办“SDK产业发展新趋势与安全实践探索”研讨会，旨在加强数字化创新的引领作用，提高数据安全的整体保障水平，为 SDK 产业有序发展建言献策。

四、SDK 合规治理建议

（一）“技管结合”保障 SDK 安全合规开发集成

“技管结合”是指将技术措施和管理策略相结合，以确保 SDK 全生命周期安全合规。二者的结合能使得企业适应快速更新的法律法规、不断变化的监管环境，有效保障和提升 SDK 全生命周期的合规治理水平，为企业的可持续发展提供坚实的基础。具体而言，“技管结合”可以包括以下方面：

1.制定内部技术标准和合规治理政策

在制度层面，不仅需要在技术层面制定相应地内部技术实施标准，对相关技术人员在开发 SDK 产品或者集成使用 SDK 产品时提出相应的技术要求，从而确保产品的安全与质量，还需要在管理层面制定合规治理政策，明确技术需要达到的合规治理效果，并明确相关人员

的职责，保障合规治理工作推进。同时，需要保证内部技术标准和合规治理政策具有一致性，不存在冲突矛盾。

2.进行风险评估与管理

风险评估的目的是确定风险的优先级，并为风险管理提供决策支持。SDK 可能引发众多安全合规风险，并且由于可能被其他产品集成使用，造成影响也更为严重、广泛，因而不论是开发还是集成使用 SDK 产品都需要对其进行风险评估。技术侧由于更了解产品的技术细节，可以更加精准识别技术安全风险。管理侧则可以根据技术侧提供的具体技术风险点制定风险管理计划和流程，同时由于对法律法规、监管政策更为熟悉，也能指导技术侧在开发使用 SDK 的过程中尽可能规避违法违规风险点。

3.建立日常监控与应急响应机制

技术侧在日常生产经营中应当对开发使用的 SDK 产品开展实时监控和日志记录，可以利用机器学习等人工智能算法辅助开展自动化、智能化故障排查和异常监测，在条件允许的情况下搭建安全合规检测平台或者使用第三方开发的平台开展日常监控，以预防安全威胁。同时针对可能造成严重后果的安全合规突发事件，技术侧应制定相关技术方案以快速响应安全突发事件，尽可能降低突发事件可能带来的危害。管理侧则需要负责协调资源和内部沟通，并制定和演练应急预案，以确保应急措施的有效性。

4.开展定期安全审计与持续改进

技术侧需要针对开发和集成使用的 SDK 产品定期进行安全漏洞

扫描，识别和评估不断迭代更新的 SDK 产品所存在的安全威胁。管理侧则需要定期开展内外部审计工作，包括技术安全审计和合规管理审计，并根据审计结果进行技术方案和管理制度的改进。

5.畅通内外部沟通反馈渠道

对内，管理侧需构建高效的内部沟通机制，及时回应各部门员工发现的 SDK 合规治理问题，并及时向主责部门传达，督促其开展后续处理。同时，技术侧和管理侧也需要加强日常沟通，管理侧应当将日常监测到的法律法规、监管实践更新情况向技术侧反馈，以帮助技术侧及时调整产品服务。对外，管理侧需建立有效用户反馈渠道，及时收集用户意见，与技术侧共同分析用户意见，提升产品安全合规性。

6.培养合规治理能力与意识

管理侧需要加强日常的合规培训和合规教育，提高员工的安全意识，将安全意识融入企业文化和日常运营，尤其需要增强与 SDK 合规治理直接相关的一线技术人员和业务人员的合规治理意识，尽可能从源头保证 SDK 的安全合规性。

（二）“多方协同”护航 SDK 行业安全合规发展

SDK 行业安全合规发展是一个系统性问题，需要“多方协同”，即相关监管机构、SDK 提供者和集成使用者、行业组织、终端用户等共同努力。

1.监管机构

监管部门可以进一步制定、完善与 SDK 相关的规则，明确 SDK

提供者和使用者的法律责任和义务，还可以推动 SDK 领域的标准化工作开展，为 SDK 的安全开发和使用提供指引。监管部门需要根据现行规定定期对 SDK 开展监督检查，并对违规行为进行通报、作出处罚，以确保 SDK 提供者和使用者合规经营。此外，监管部门还可以主动促进 SDK 提供者、使用者以及相关组织之间的沟通协作，共同提高 SDK 合规治理水平。

2.SDK 提供者和集成使用者

SDK 提供者和 SDK 集成者在日常经营中，必须重视 SDK 开发和集成使用安全，采取“技管结合”的方式保障 SDK 安全合规。对于最为频发的个人信息安全合规问题，SDK 提供者和使用者应当共同协作，通过提供合规指引、开展合规审查等方式，提升 SDK 的个人信息保护能力。

3.行业组织

行业组织可以积极与监管部门合作，参与制定关于 SDK 安全的政策法规，反映行业需求并提供专业建议。行业组织还可以自行牵头制定和推广 SDK 开发和集成的安全标准，为企业提供统一的安全实践指南。并且，为了更好地帮助企业验证其产品是否符合安全标准和法规政策要求，行业组织也可以向企业积极提供 SDK 安全评估和认证服务。此外，行业组织可以组织培训课程和提供教育资源，建立平台促进成员之间的信息共享，帮助企业了解行业内最新的 SDK 合规治理最佳实践。

4. 终端用户

终端用户需要不断增强对个人信息保护等安全意识，了解 SDK 可能带来的安全合规风险，并尽可能通过阅读隐私政策、审慎授权、定期更新所使用产品等方式保护自己的人身财产安全。同时，终端用户作为 SDK 相关产品的直接使用者，在使用过程中，如果发现 SDK 存在违规行为和安全风险，可以积极向 SDK 提供者、SDK 集成者或有关监管部门反馈。

中国信息通信研究院 知识产权与创新发展中心

地址：北京市海淀区花园北路 52 号

邮编：100191

电话：010-62309801

传真：010-62301252

网址：www.caict.ac.cn