汉坤法律评述

2021 年 4 月 26 日

HANKUN
汉 坤 律 师 事 务 所
Han Kun Law Offices

北京 | 上海 | 深圳 | 香港

简评《移动互联网应用程序个人信息保护暂行规定》（征求意见稿）

作者：段志超 | 蔡克蒙 | 王雨婷 | 胡敏喆

2021 年 4 月 26 日，工业和信息化部公布在国家互联网信息办公室的统筹指导下，工信部会同公安部、市场监管总局起草的《移动互联网应用程序个人信息保护暂行规定》（征求意见稿），并向社会公开征求意见（简称“**规定征求意见稿**”）。规定征求意见稿总结和提炼了近两年前述四部委特别是工信部在《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 APP 侵害用户权益专项整治行动》（工信部信管函〔2019〕337 号）、《关于纵深推进 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）等一系列 APP 个人信息保护整治行动中提出的要求和措施，勾勒出了我国 APP 个人信息保护领域的制度框架。

值得注意的是，规定征求意见稿针对 APP 开发运营者、APP 分发平台、APP 第三方服务提供者、移动智能终端生产企业和网络接入服务提供者明确了不同的合规义务，且明确了相应的整改期限和责任。一旦发现违规，相关主体又没有在 5 个工作日内完成整改的，即面临处罚风险，持续逾期未完成整改的，甚至面临下架以及断开接入的后果。在规定创设的立体化监管下，相关主体应将个人信息合规工作常态化和制度化，避免一旦触发整改义务后猝不及防，造成对日常运营的负面影响。

一、适用范围

规定适用于在中华人民共和国境内开展的 APP 个人信息处理活动。APP 个人信息处理活动是指“移动智能终端中运行的应用程序收集、存储、使用、加工、传输个人信息的活动”。这一概念的外延比较广泛，可以涵盖手机设备预置 APP、通过应用商店安装使用的 APP 以及通过其他应用平台在线使用的小程序。

二、知情同意

规定征求意见稿系统性地规定了 APP 收集个人信息各环节的知情同意要求，主要包括：

- 在 APP 注册登录及首次运行环节，通过弹窗、文本链接及附件等方式，告知用户个人信息处理主体、处理目的、处理方式、处理类型、保存期限等个人信息处理规则，并通过非默认勾选的方式征得用户同意。在实践中，APP 开发运营者应在启动后首页设置并展示 APP 个人信息保护政策弹窗，并确保在用户勾选或点击确认隐私政策前不收集任何用户个人信息。

- 未经用户同意，APP 不得更改用户设置的权限状态。APP 向用户申请所需权限必须具备具体业务功能需求，在对应业务功能启动时向用户申请相应权限，而不应强迫用户在 APP 启用环节一揽子同意打开多项系统权限。在实践操作中，APP 应在相关业务功能需开启系统权限时，通过可编辑系统弹窗或 APP 弹窗（如系统弹窗无法编辑）向用户告知权限开启目的及收集的个人信息，并征得用户主动点击同意。

- APP 向 APP 外第三方提供个人信息，应告知用户第三方的身份、联系方式、处理目的、处理方式和个人信息的种类等事项，并取得用户的同意。此前四部委出台的《APP 违法违规收集使用个人信息行为认定方法》已经要求 APP 在隐私政策中逐一列明 APP 委托的第三方或嵌入的第三方代码、插件收集使用个人信息的目的、方式、范围。监管机构在根据认定办法开展的执法活动中，重点关注 APP 是否逐一披露第三方 SDK 的个人信息收集使用情况。而相较认定办法，规定征求意见稿中“第三方”的范围可能更加宽泛。该概念是否应等同于规定征求意见稿中界定的“APP 第三方服务提供者”，即“相对于用户和 APP 以外的，为 APP 提供软件开发工具包（SDK）、封装、加固、编译环境等第三方服务的主体”，还是亦应包括“APP 第三方服务提供者”之外的通过其他线上线下方式获得 APP 个人信息的第三方，有待在实践中进一步观察。

- 处理种族、民族、宗教信仰、个人生物特征、医疗健康、金融账户、个人行踪等敏感个人信息的，应当对用户进行单独告知，取得用户同意。在实践中，APP 在收集上述个人敏感信息前，应在收集页面同步告知用户信息收集目的，用户主动提交上述个人信息敏感信息可视为其同意信息的收集。

三、最小必要

在落实“最小必要”原则方面，规定征求意见稿强调：

- 处理个人信息应遵循最小必要原则，不得处理与服务场景无关的个人信息；在非服务所必需或无合理场景下，不得自启动或关联启动其他 APP。

- 处理个人信息的数量、频次、精度等应为服务所必需。

- 用户拒绝提供非服务所必需的个人信息或权限后，不得拒绝用户使用服务或频繁请求用户开启权限干扰用户正常使用服务。

- 不得以改善服务质量、提升使用体验、研发新产品、定向推送信息、风险控制等为由，强制要求用户同意超范围或与场景无关的个人信息处理。

APP 开发运营者落实上述要求过程中应注意以下要点：

- APP 开发运营者可参考《常见类型移动互联网应用程序必要个人信息范围规定》、《APP 收集使用个人信息最小必要评估规范》等规范和标准，结合具体使用场景，确定各类型服务所需必要个人信息的范围、精度，获取个人信息所需调用权限的前台调用频次、后台运行或静默状态调用频次等。

- 信息安全标准化委员会此前制定的《网络安全标准实践指南 — 移动互联网应用程序（APP）个人信息保护常见问题及处置指南》（TC260-PG-20203A）对频繁申请系统权限干扰用户正常使用提出了量化标准，包括（1）单个场景在用户拒绝权限后，48 小时内弹窗提示用户打开系统权限的次数

超过 1 次；（2）每次重新打开 APP 或使用某一业务功能时，都会向用户索要或提示用户缺少相关系统权限。

- 在实践中，“改善服务质量、提升使用体验、研发新产品、定向推送信息、风险控制”等是常见的个人信息收集或使用理由。目前实践中 APP 运营者一般会在个人信息保护政策告知上述收集目的，通过用户接受隐私政策“一揽子”获得用户同意，而不会为用户提供选择是否允许为上述目的收集个人信息的单独同意机制。我们认为规定征求意见稿并未一概否认为上述目的收集使用个人信息的正当性，而是强调为前述目的收集个人信息应与具体应用场景具有相关性。

四、数据治理与安全保护

规定征求意见稿还对 APP 开发运营者的数据治理与安全保护义务做出了规定，主要包括：

- 将个人信息保护要求贯穿 APP 设计、开发及运营环节。这一规定体现了近年来国际上流行的隐私设计理念（privacy by design），亦是首次将隐私设计上升到法规层面要求。
- 提高透明度，以显著清晰的方式定期向用户呈现 APP 的个人信息收集使用情况。这意味着 APP 开发运营者告知个人信息处理规则的义务不再是一次性的，不限于首次告知或在变更时告知，而是应定期告知。具体告知呈现的方式还有待产品和法律相关从业人士进一步探索。
- 基于个人信息向用户提供商品或服务的搜索结果的，应当保证结果公平合理，同时提供不针对其个人特征的选项。规定征求意见稿在此专门强调结果公平合理，体现了监管机构对基于个人信息的歧视性待遇、大数据杀熟等热点问题的关切。
- 通过制定管理规则、签署协议等方式加强对涉及个人信息处理的第三方服务的监督管理。
- 不得通过绑定相互独立的服务功能模块，扩大个人信息收集的范围与数量，强制收集个人信息。
- 加强 APP 前端和后端安全防护、访问控制、技术加密、安全审计、个人信息泄露监控与应急处置。
- 需要认证用户真实身份信息的，应当通过国家统一建设的公民身份认证基础设施所提供的网上公民身份核验认证服务进行。

五、全流程立体化监管

规定征求意见稿还明确了 APP 的分发、预置安装、网络接入、第三方服务接入全流程的个人信息保护审核、透明度与安全保障义务，加强对 APP 个人信息保护的规范：

- APP 分发平台[1]应在 APP 上架前严格审核管理分发的 APP，并在规定出台后 1 个月内对已经上架的 APP 进行补充审核。APP 应用分发平台应向用户提示所分发 APP 收集使用个人信息情况，并按照监管要求及时处置违规 APP。APP 分发平台还应设置便捷的投诉举报入口，及时处理公众关于 APP 违规处理个人信息行为的举报。

[1] APP 分发平台指网站、应用商店、APP 等提供 APP 下载、安装、升级的应用软件平台（可包括微信、百度、支付宝等小程序开发平台）。

- APP 第三方服务提供者[2]应加强个人信息收集使用情况的透明度，制定公布个人信息处理规则，不得未经用户同意隐秘收集用户个人信息，或在无合理应用场景下收集个人信息。未经用户同意不得进一步共享转让收集到的用户个人信息。APP 第三方服务提供者还应在发现安全风险或者个人信息处理规则变更时及时更新并告知 APP 开发运营者。

- 移动智能终端生产企业[3]应加强终端系统权限管理能力，记录并通过明显方式告知用户 APP 获取和使用系统敏感权限情况，还应建立重点 APP 关注名单，加强预置审核，并完善终端设备身份管控机制。规定征求意见稿还特别强调移动智能终端生产企业应完善终端设备标识管理能力，这意味着后续移动智能终端生产企业可能需要进一步加强 APP 对设备标识符获取的限制，强化用户对唯一标识符获取、重置等方面的控制力。

- 网络接入服务提供者[4]应登记并核验 APP 运营者真实身份，联系方式，并按电信管理机构要求及时对违规 APP 采取停止接入等必要措施。

规定征求意见稿明确监管机构有权责令检测发现问题的 APP 在 5 个工作日完成整改，5 个工作日内未完成整改，监管机构可依法向社会公告，如公告后 5 个工作日内仍未完成整改，监管机构可要求 APP 分发平台下架相关 APP。下架后仍未完成整改，将对 APP 采取断开接入等必要措施。被下架的 APP 在 40 个工作日内不得通过任何渠道再次上架，且 APP 开发运营者申请 APP 再次上架，需完善技术与管理措施，做出企业自律承诺后，并向要求下架的监管部门提出申请。被断开接入的 APP 重新接入亦需向要求断开的监管部门提出申请。对整改反复出现问题的 APP 及其开发运营者开发的相关 APP，监管部门可以指导组织 APP 分发平台和移动智能终端生产企业在集成、分发、预置和安装等环节进行风险提示，情节严重的采取禁入措施。

六、建议

规定总结提炼了我国此前一个阶段的 APP 个人信息治理工作的核心制度框架。对于违规 APP 监督检测，规范祭出了监管机构检查、第三方机构检测、用户投诉举报、APP 分发平台审核处置、移动智能终端生产企业权限管理与重点监测、网络接入服务提供者终止接入的“组合拳”，而一旦被发现违规责令整改，APP 开发运营者必须在短短 5 个工作日内完成整改，时间压力巨大。因此，APP 开发运营者必须重视 APP 个人信息保护日常合规工作，做到未雨绸缪。幸运的是此前监管机构已经发布了一系列规范和标准，可以为 APP 运营者及相关从业人员开展 APP 个人信息合规自查提供有效指引。特别值得关注的是，日前信息安全标准化委员会发布的《信息安全技术 移动互联网应用程序（APP）个人信息安全测评规范》（征求意见稿）对第三方测评机构对 APP 个人信息安全进行测评的方式、流程与标准做出指引，该规范有助于 APP 运营者了解第三方机构的测评方式、流程与要点，并相应提前开展自查与整改工作，防患于未然。

[2] APP 第三方服务提供者指相对于用户和 APP 以外的，为 APP 提供软件开发工具包（SDK）、加固、编译环境等第三方服务的主体。

[3] 移动智能终端生产企业指生产能够接入公众网络，提供预置 APP 或者具备安装 APP 能力的移动智能终端设备的主体。

[4] 网络接入服务提供者指从事互联网数据中心（IDC）业务、互联网接入服务（ISP）业务和内容分发网络（CDN）业务，为 APP 提供网络接入服务的电信业务经营者。

特别声明

汉坤律师事务所编写《汉坤法律评述》的目的仅为帮助客户及时了解中国或其他相关司法管辖区法律及实务的最新动态和发展，仅供参考，不应被视为任何意义上的法律意见或法律依据。

如您对本期《汉坤法律评述》内容有任何问题或建议，请与汉坤律师事务所以下人员联系：

段志超

电话： +86 10 8516 4123
Email： kevin.duan@hankunlaw.com