君合研究简讯

JUNHE

2020 年 4 月 15 日

信息保护和网络安全法律热点问题

App 个人信息保护又添新规——信标委发布两份最新文件征求意见

近日，全国信息安全标准化技术委员会（简称“**信标委**”）分别于 3 月 19 日与 3 月 30 日先后发布了《网络安全标准实践指南—移动互联网应用程序（App）收集使用个人信息自评估指南》（简称“**《自评估指南》**”）与《网络安全标准实践指南—移动互联网应用程序（App）个人信息安全防范指引》（简称“**《安全防范指引》**”）两份文件的征求意见稿，旨在为 App 运营者提供自我纠察的评估要点和隐私实践的合规指引。两份文件已分别于 4 月 2 日及 4 月 13 日前完成公开意见征集。

一、背景

近年来，针对 APP 违法违规收集个人信息的现象，已有多部规定和标准出台，例如：

(1) 2019年1月23日四部委发布的《关于开展App违法违规收集使用个人信息专项治理的公告》[1]；

(2) 2019年3月3日四部委发布的《App违法违规使用个人信息自评估指南》[2]；

(3) 2019年3月13日市场监督管理总局、中央网信办发布的《关于开展App安全认证的公告》[3]；

(4) 2019年12月30日四部委发布的《App违法违规收集使用个人信息行为认定方法》[4]；

(5) 2020年1月20日信标委发布的《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》（草案）[5]。

多家政府部门针对 APP 违法违规收集个人信息根据上述规范密集执法，实践之中企业不断进行相应整改，以符合监管要求。

与上述规定相比，《自评估指南》与《安全防范指引》两份文件征求意见稿的主要要求并无重大实质变化，但在总结前述文件实践经验的基础上，立足具体场景与示例，提出了更为细致的指引。

二、《自评估指南》重点新增内容

《自评估指南》沿袭了此前许多细节的评估要点并提出具体标准，其中，下述新增或再次强调内容值得关注。

1、 如果存在个人信息出境情形，《自评估指南》进一步要求，隐私政策中应将出境个人信息类型逐项列出并显著标识（如字体加粗、标星号、下划线、斜体、不同颜色等）；如果不存在个人信息出境情形，则明确说明。

2、 对于之前作为执法重点的 SDK 问题，《自评估指南》再次强调，嵌入第三方代码或插件，应说明第三方类型及个人信息收集的相关信息，若第三方或其嵌入的代码、插件将个人信息传输至境外，应向用户明确说明。

《自评估指南》将相关要求标准进一步细化，例

1 http://www.cac.gov.cn/2019-05/23/c_1124532020.htm
2 https://mp.weixin.qq.com/s/u2XZn02SJkOvzeNSdzJiEA
3 http://www.gov.cn/xinwen/2019-03/15/content_5373928.htm
4 http://www.cac.gov.cn/2019-12/27/c_1578986455686625.htm
5https://www.tc260.org.cn/front/bzzqyjDetail.html?id=20200121161345843731&norm_id=20200116010001&recode_id=36736

如：

- 用户明确拒绝后，不得向用户频繁（如 48 小时内）询问是否同意收集个人信息或相关权限；用户选择使用 App 某一具体功能触发征得同意的动作，不属于频繁干扰情形。
- App 不得以捆绑方式强制要求用户一次性同意打开多个可收集个人信息权限。如将安卓版 App 的 targetSdkVersion 值设置低于 23，通过声明机制，在安装 App 时要求用户一次性同意打开多个可收集个人信息权限。
- 在要求用户提供个人敏感信息时，App 应通过显著方式（如弹窗提示、文字备注、文本链接等）同步告知用户其目的，对目的的描述应明确、易懂。

三、《安全防范指引》重点新增内容

《安全防范指引》以问题为导向，立足于 App 业务实践中存在的、常见的违法违规收集使用个人信息的十个问题，例如超范围收集、无法注销或设置不合理条件、强制捆绑销售等，通过场景化分析提出了针对性的企业合规措施。《安全防范指引》中的新增内容和值得注意的要点包括：

1、 在摘要中规定“建议 APP（含小程序）运营者参考本实践指南”。首次将小程序纳入到《安全防范指引》等 APP 指南的适用范畴；

2、 提出 APP 应尽量避免收集不可变更的设备唯一标识，如 IMEI 号、MAC 地址等，用户保障网络安全和运营安全的除外。

另外，《安全规范指引》结合当前疫情防控工作，对疫情防控 APP 收集使用个人信息提出了具体的要求。包括：

- 坚持收集个人信息的最小范围原则，收集身份登记信息达到可追溯目的即可；
- 疫情结束后应及时删除或依法处置个人信息；
- 公开隐私政策；
- 收集个人敏感信息，应同步告知用户使用目的；
- 通过个人信息的大数据分析等自动化决策机制来判断用户个人健康状态的疫情防控 APP，应提供反馈渠道、及时处理因自动化决策机制而严重影响用户个人权益的问题等。

四、我们的观察

鉴于《网络安全法》等法律、法规对个人信息保护的规定较为笼统，各政府部门及标准制定机构制定了一系列实施细则、标准及实践指南。

《自评估指南》与《安全防范指引》所属的《网络安全标准实践指南》系列标准是由信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[6]。

值得注意的是，《自评估指南》与《安全防范指引》不仅是对法律法规、国家标准文本的拓展与落实，而且是对 2019 年以来实践执法经验总结，具有相应的实操性。尽管在内容上没有重大实质变化，《自评估指南》与《安全防范指引》的出台反映出监管部门对 App 个人信息违法违规收集行为监管驱严、精细化的总体趋势。

目前，监管部门是否会在执法活动中参考这两项规定的要求有待观察，我们建议公司根据相关指引进行更为细致的自评估以做相关准备。另外，在目前为疫情收集和处理个人信息丰富和密集的情况下，我们也注意到关于加快个人信息保护法出台的呼声，这些细节指引也将为未来的个人信息法提供相应的参考。

---

6 《网络安全标准实践指南管理办法（暂行）（信安标委，2019 年）第二条。

董　潇　合伙人　电话：86 010 8519 1718　邮箱地址：dongx@junhe.com
郭静荷　律　师　电话：86 010 8553 7947　邮箱地址：guojh@junhe.com
董俊杰　律　师　电话：86 010 8540 8722　邮箱地址：dongjj@junhe.com