汉坤法律评述
2022 年 5 月 5 日

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

北京 | 上海 | 深圳 | 海口 | 香港

《信息安全技术 移动互联网应用程序（App）收集个人信息基本要求》要点解析

作者：段志超 | 蔡克蒙 | 胡敏喆[1]

2022 年 4 月 15 日，国家市场监督总局、国家标准化管理委员会发布公告，正式发布《信息安全技术 移动互联网应用程序（App）收集个人信息基本要求（GB/T 41391-2022）》（“**《基本要求》**”）。《基本要求》综合了《App 违法违规收集使用个人信息行为认定方法》《常见类型移动互联网应用程序必要个人信息范围规定》《信息安全技术 个人信息安全规范（GB/T35273-2020）》等现行法规和国家标准的规定，总结了近两年 App 信息收集监管实践和试点政策（如“**双清单**”）要求，并在细节处不乏新规亮点。本文将简要总结《基本要求》要点特别是新亮点，供企业合规工作参考。

一、《基本要求》的适用范围

《基本要求》适用于移动互联网应用程序（“**App**”）运营者规范其个人信息收集活动，包括移动智能终端预置、下载安装的应用程序和小程序。《基本要求》明确适用于“小程序”。“小程序”指基于应用程序开放接口实现的，用户无需安装即可使用的移动互联网应用程序。

二、App 可以收集哪些个人信息

《基本要求》规定，App 可收集的个人信息分为“必要个人信息”以及“非必要但有关联个人信息”。《基本要求》将二者视为与 App 提供服务目的有直接关联的个人信息，统称为“相关个人信息”。

- “必要个人信息”指保障 App 基本业务功能正常运行所必需的个人信息，缺少该信息 App 即无法实现其基本业务功能。
- “非必要但有关联个人信息”系《基本要求》新定义的概念，指与 App 所提供服务相关但可选收集的个人信息，包括基本业务功能可选收集的个人信息，以及扩展业务功能收集的个人信息。

与“相关个人信息”相对应，《基本要求》还规定了“无关个人信息”，即与 App 所提供服务目的无直接关联的个人信息，即没有该等个人信息的参与，对于该 App 提供的任何一项业务功能的正常实现和服务质量没有影响。《基本要求》认为 App 不应收集、也不应向用户征求同意收集“无关个人信息”。

[1] 实习生金今对本文的写作亦有贡献。

三、如何确定“必要个人信息”的范围？

如果 App 类型属于附录 A 给出的常见服务类型，应按照附录 A 中所对应的服务类型确定 App 的必要个人信息范围。附录 A“常见服务类型 App 必要个人信息范围及使用要求”整体沿用了此前《常见类型移动互联网应用程序必要个人信息范围规定》所规定的常见服务 App 的类型及相关类型 App 必要个人信息的范围，但在《规定》的基础上进一步细化了一些特定服务类型 App 的必要个人信息使用要求。例如“地图导航”类 App 收集使用位置信息，仅能用于确定用户位置，提供地图搜索展示和导航服务，导航场景下持续定位获得的行踪轨迹仅能用于本次线路导航，完成导航后应及时删除或匿名化处理。

当 App 类型不属于附录 A 给出的常见服务类型时，应当划分该 App 的基本业务功能和扩展业务功能，再将保障 App 基本业务功能正常运行所必需的个人信息确定为必要个人信息。

四、如何确定基本业务功能和扩展业务功能？

区分基本业务功能和扩展业务功能的主要意义在于确定必要个人信息的范围。基本业务功能与扩展业务功能应按照如下方式确定：

(1) 基本业务功能的界定基本延续了《信息安全技术 个人信息安全规范（GB/T35273-2020）》的规定：

- 实现用户主要使用目的的业务功能所属服务类型为该 App 的类型；
- 当 App 类型属于附录 A 给出的常见服务类型时，应按照附录 A 对应的服务类型划分为 App 的基本业务功能；
- 当 App 类型不属于附录 A 给出的常见服务类型时，应将实现用户主要使用目的的业务功能划分为 App 的基本业务功能。

(2) 扩展业务功能是基本业务功能之外的其他业务功能。《基本要求》还明确：

- 对于提供多种服务类型的 App 而言，App 功能类型之外的其他服务类型属于扩展业务功能；
- 仅为实现改善服务质量、提升使用体验、定向推送信息、研发新产品等目的的业务功能应划分为扩展业务功能；
- 外部第三方或关联公司提供的业务功能原则上应划分为扩展业务功能；
- 基本业务功能因技术发展而出现的新实现方式，如新方式相较传统方式收集更为敏感的个人信息，对个人权益影响更大，可视为扩展业务功能，通常作为基本业务功能的可选替代、补充使用。

五、收集个人信息的要求

《基本要求》延续了现行规定中 App 个人信息收集的基本要求，包括具备明确、合理、具体的处理目的，范围限于实现处理目的最小必要、与目的直接相关，采取对个人权益影响最小的方式收集，应采取弹窗、图文等显著方式告知用户个人信息保护政策的核心内容，并取得用户明示同意。在此基础上，《基本要求》特别强调应向用户明示 App 基本业务功能、扩展业务功能和必要个人信息范围，显著区分必要和非必要个人信息，并拆分必要个人信息和非必要个人信息的同意。如果无需收集个人信息即可提供 App 基本业务功能，应确保用户在不提供个人信息的情况下可正常使用 App 基本业务功能。

App 收集“非必要个人信息”（实际是指“非必要但有关联个人信息”）需遵守诸多额外的限制条件，主要包括：

- 保障用户可以拒绝或撤回同意，且不得因用户拒绝或撤回同意提供非必要个人信息，而拒绝用户使用该 App 的基本业务功能。如果非必要个人信息系提供扩展业务功能所需，拒绝或撤回同意可通过用户关闭、退出扩展业务功能实现（前提是不影响用户使用基本业务功能）；
- 不得通过捆绑基本业务功能和扩展业务功能、批量申请授权等，强迫用户同意收集非必要个人信息的请求；
- 当 App 提供多种服务类型时，应按照服务类型制定个人信息保护政策，按照服务类型分别向用户申请处理个人信息的同意。App 类型之外的其他服务类型[2]，宜由用户自主选择启用。当用户首次使用时，宜采取增强式告知方式明示该服务类型的个人信息处理规则，并取得用户明示同意。

根据上述要求，由于 App 基本业务功能及必要个人信息的范围被严格限制，而扩展业务功能和非必要个人信息需要用户主动启用，获得用户明示同意，且不同意不得影响用户使用基本业务功能，因此未来 App 隐私政策在获得用户同意方面的作用将进一步弱化，仅起到告知用户的作用，或至多作为获得基础业务功能所需的必要个人信息的同意机制，不同意隐私政策不让用 App 将面临更高的合规风险。App 需开发“基础版本”、“浏览模式”等，使用户可以在拒绝隐私政策的情况下，仍可使用无需收集个人信息或仅收集必要个人信息的基础业务功能。

六、App 涉及个人信息收集的系统权限申请和使用方面的要求

《基本要求》在涉及个人信息收集的系统权限申请和使用方面基本延续了《TC260-PG-20204A 网络安全实践指南—移动互联网应用程序（App）系统权限申请使用指引》（“**《指引》**”）所规定的最小必要、用户可知、不强制不捆绑、动态申请等原则及具体权限申请要求。《基本要求》还在《指引》的基础上明确 App 通过权限获得的个人信息和能力，不应在未经用户同意的情况下提供给 App 接入的第三方应用或嵌入的第三方 SDK 使用。换言之，如 SDK 申请收集个人信息的系统权限或 App 将通过系统权限收集的个人信息提供给第三方 SDK，应获得用户同意，但是否必需为单独同意仍有待在实践中进一步明确。

七、App 应如何管理第三方应用和第三方 SDK

《基本要求》区分了第三方应用和第三方 SDK。《基本要求》所规定的第三方应用指通过移动互联网应用程序面向用户提供服务的应用程序，提供形式包括小程序、Web 页面，以及直接向用户提供服务的 SDK 等。而如果 SDK 不直接向用户提供服务，则作为第三方 SDK 而非第三方应用进行管理。《基本要求》要求 App 对第三方进行事前安全性审查和评估、与第三方约定双方个人信息处理规则和保护责任、明确第三方协助 App 响应用户权利请求的措施、事中事后持续监督第三方个人信息安全管理情况并在必要时停止接入违规第三方。对二者管理的差异在于，《基本要求》所规定的第三方应用更接近独立的个人信息处理者，虽强调 App 需提示用户注意第三方个人信息处理规则、确保用户便捷授权或撤回授权第三方应用收集个人信息或向第三方应用提供个人信息，但总体而言 App 的责任相对较低；而对第三方 SDK，由于其不直接向用户提供服务，更偏向后台端，因此 App 的管理责任较高，需自行告知用户第三方 SDK 处理个人信息、申请系

[2] App 类型之外的其他服务类型属于扩展业务功能，因此收集的相关个人信息也属于“非必要个人信息”。

统权限的情况，对 SDK 权限申请和使用、是否存在自启动、关联启动、是否涉及向境外提供个人信息、是否存在热更新机制等进行事先审核和事中事后监督。

值得注意的是，《基本要求》明确规定如果第三方应用或第三方 SDK 由集团内关联公司提供，则原则上按照第三方进行管理。但如果该等集团内关联方与 App 运营者遵守同一套管理制度、统一进行安全和运维管理，则不属于 App 运营者的第三方。这一规定为实践中颇具争议的集团内不同主体间共享个人信息提供了一定空间。

八、定向推送信息和用户画像场景应收集可重置唯一设备标识符

在定向推送信息和用户画像场景采用唯一设备识别码标识用户时，应使用可变更的唯一设备识别码（即可重置的标识符，如 AAID、IDFA、随机 MAC 地址等），且不应将其与用户信息或不可变更的唯一设备识别码关联。常见不可变更的唯一设备识别码包括 IMEI、IMSI、MEID、MAC 地址、SN、ICCID（SIM Serial Number），但不包括随机化处理后的 MAC 地址。然而，《基本要求》并未像《TC260-PG-20204A 网络安全实践指南—移动互联网应用程序（App）系统权限申请使用指引》一样明确是否可以基于安全风控目的收集不可变的唯一设备识别码。

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

蔡克蒙

电话： +86 10 8516 4289
Email： kemeng.cai@hankunlaw.com