国家标准《信息安全技术 移动智能终端的移动互联网应用程序（App）个人信息处理活动管理指南》（征求意见稿）编制说明

一、工作简况

1、任务来源

根据国家标准化管理委员会2021年下达的国家标准制修订计划，《信息安全技术 移动智能终端的移动互联网应用程序（App）个人信息处理活动管理指南》由华为技术有限公司承办，计划号：XXXXXXXX-T-469。该标准由全国信息安全标准化技术委员会归口管理。

2、标准编制的主要成员单位

华为技术有限公司负责起草，中国电子技术标准化研究院、中国网络安全审查技术与认证中心、OPPO广东移动通信有限公司、维沃移动通信有限公司、北京小米移动软件有限公司、荣耀终端有限公司、北京三星通信技术研究有限公司等单位共同参与了该标准的起草工作。

3、主要工作过程

2020 年 12 月，撰写组成立，召开第一次小组讨论会，明确本规范对象和主要内容，确定了以移动终端操作系统为对象，以操作系统上涉及的 APP 收集使用个人信息相关管控为主要内容，并分配了相关工作。

2021 年 1 月，编制组在“四部委 APP 治理小组”的工作基础上，分析 APP 在个人信息保护方面常见问题，梳理出可通过操作系统增强的问题点；分析、梳理近年来主流操作系统在个人信息保护方面的增强点。

2021 年 3 月，起草标准草案。

2021 年 8 月 15 日，华为技术有限公司、中国电子技术标准化研究院、中国网络安全审查技术与认证中心等共同组成标准编制组，召开该标准编制启动工作会议。会上讨论了对标准撰写思路的想法和意见；

2021 年 9 月至 11 月，标准编制组讨论并修改国家标准《信息安全技术 移动智能终端的移动互联网应用程序（App）个人信息处理活动管理指南》（草案）；

2021 年 11 月 11 日，TC260 SWG-BDS 工作组在北京组织召开了组内专家评审会。专家组听取了标准编制组的工作汇报，审阅了相关文档，质询了有关问题。

2021 年 12 月至 2022 年 3 月，根据 2021 年第二次会议讨论意见、以及编制组成员线下反馈意见形成征求意见稿，并组织编制组成员讨论征求意见稿。

2022 年 4 月 14 日，TC260 组织专家进行了标准征求意见稿评审，根据专家意见对用户展示 app 个人信息处理等内容进一步细化，有利于用户进行查看与管理。

2022 年 5 月，根据专家以及编制组成员会议讨论意见进行修改完善，形成最终征求意见稿。

二、标准编制原则和确定主要内容的论据及解决的主要问题

1、编制原则

本标准的编制原则是：

1）通用性

按照本标准实现的移动智能终端的App个人信息处理活动管理指南，可实现基本技术规格一致，便于用户使用和管理。

2）实用性

根据我国国情、实际运用环境和国家有关政策编制本标准，使其在指导移动智能终端的App个人信息处理活动管理，保障个人信息安全方面具有很强的实用性。

3）安全性与隐私

在本标准中对移动智能终端的App个人信息处理活动的数据安全与隐私做了实施指南，从而确保个人信息处理活动管理过程中的安全性。

4）符合性

符合国家有关法律法规和已有标准规范的相关要求。

2、确定主要内容的依据

标准制定的依据为：

a）标准格式按照 GB/T 1.1—2020 标准要求编写。

b）本标准制定参考以下国家、行业标准：

GB/T 35273—2020 信息安全技术 个人信息安全规范

GB/T 39335—2020 信息安全技术 个人信息安全影响评估指南

3、解决的主要问题

本标准应用在移动终端操作系统在 APP 收集、使用个人信息时提供管理、提示、控制等功能，例如针对敏感个人信息或移动终端敏感能力，提供更强的提醒机制，为用户提供应用软件调用行为记录，针对系统提供的存储能力给出优化的管控机制，避免应用软件生成的信息被其它应用软件获取，针对权限管理，给出优化的授权范围、授权方式，以控制应用软件获得个人信息的内容或频率。

本标准适用于移动终端生产、制造企业在实践中提高个人信息保护能力，本标准将首先在牵头公司中进行应用试点，并逐渐推广到其它终端厂家。

目前，由于相关标准规范缺失，移动智能终端的 App 个人信息处理活动在数据滥采、存储、使用方面没有明确的安全要求，造成安全防护措施薄弱，未经用户明确授权或超范围使用个人信息的情况普遍存在挑战。

本标准拟提出移动智能终端的 App 个人信息处理活动要求，标准主要框架基于 APP 在移动智能终端的生命周期各节点中用户个人信息风险，给出 APP 各生命周期移动终端的管理措施，具体包括：安装阶段措施、启动阶段措施、运行阶段措施、更新阶段措施、退出、卸载阶段措施，其中 APP 运行涉及到个人信息处理的场景最多，因此此阶段又包括了 APP 使用个人信息提示、APP 调用个人信息行为记录、设备识别码访问控制、敏感数据访问控制、存储空间使用、系统权限能力增强几个方面措施。

三、主要试验情况分析

对行业标准进行调研分析，对国内厂商的主流产品进行充分调研，在尽量广泛的生产厂家范围内提高征求意见，为试验验证作基础。

四、知识产权情况说明

本标准不涉及专利及知识产权问题。

五、产业化情况、推广应用论证和预期达到的经济效果

移动智能终端的 App 个人信息处理活动标准化对于增强我国各相关行业信息安全，尤其是个人信息安全具有重要意义。移动智能终端的 App 个人信息可能被检索或分析，如数据主体的财务状况或推断健康信息、位置信息等。App 个人信息可能被滥用于其他目的，并被数据收集者所滥用。

六、采用国际标准和国外先进标准情况

本标准为自主制定，结合我国针对 App 个人信息保护的要求，能够为我国 App 个人信息处理活动提供管理指南。

七、与现行相关法律、法规、规章及相关标准的协调性

本标准与现行法律、法规协调一致，《个人信息保护法》第七条要求“处理个人信息应当遵循公开、透明原则”，本标准面向移动互联网 APP，以移动智能终端，主要是智能手机为对象，为 APP 实现公开、透明原则提供终端系统层面的技术保障。

本标准与现行强制性国家标准及相关标准协调一致。本标准在同 GB/T 35273—2020 《信息安全技术 个人信息安全规范》、GB/T 39335—2020 《信息安全技术 个人信息安全影响评估指南》、GB/T 40660—2021 《信息安全技术 生物特征识别信息保护基本要求》协调一致基础上，针对 App 个人信息处理活动的细化与补充，并提出针对性的具体安全要求。

八、重大分歧意见的处理经过和依据

无。

九、标准性质的建议

建议作为国家推荐性标准发布。

十、贯彻标准的要求和措施建议

本标准主要用于通过标准化的形式来将移动智能终端的 App 个人信息处理活动等进行规范，有助于促进和规范当前移动智能终端的 App 个人信息保护工作的推进和管理。

十一、替代或废止现行相关标准的建议

无。

十二、其它应予说明的事项

无

《信息安全技术 移动智能终端的移动互联网应用程序（App）个人信息处理活动管理指南》编制工作组

2022-6