ICS 33.050
M 30

团　体　标　准

T/TAF XXX-XXXX

移动智能终端与应用软件用户个人信息保护实施指南 第1部分：总则

User personal information protection implementation guide on mobile intelligent terminal and application software Part 1: General principle

目　　次

前　言

标准按照 GB/T 1.1-2009 给出的规则起草。

本标准中的某些内容可能涉及专利。本标准的发布机构不承担识别这些专利的责任。

本标准由电信终端产业协会提出并归口。

本标准起草单位：中国信息通信研究院、华为技术有限公司、OPPO广东移动通信有限公司、维沃移动通信有限公司、武汉安天信息技术有限责任公司、北京奇虎科技有限公司

本标准主要起草人：宁华、衣强、王艳红、李腾、贾科、姚一楠、罗成、黄莹、杜云、周飞、邓佑军、余泉、王浩迁。

引　　言

近十年智能终端的普及，也带动了其上与移动应用的蓬勃发展，在移动终端和应用软件大发展的潮流下，个人信息违规收集、滥用等现象严重，危害了个人信息主体权益，个人信息保护实施指南系列标准旨在规范移动终端和应用软件中个人信息管理的重点环节的操作，本规范作为个人信息保护实施指南系列标准的总则，给出个人信息保护总体思想，对个人信息保护实施指南系列标准起着提纲挈领的作用。

移动智能终端与应用软件用户个人信息保护实施指南 第1部分：总则

1 范围

本标准给出移动终端和应用软件上用户个人信息生命周期，以及给出生命周期各阶段要求，是移动终端和应用软件个人信息保护系列标准或其它与移动终端数据相关标准的参考。

本标准适用于各种制式的移动智能终端及移动终端上的应用软件，个别条款不适用于特殊行业、专业应用，其他终端也可参考使用。

2 规范性引用文件

GB/T 35273-2020 《个人信息安全规范》
YD/T 2407-2013 《移动智能终端安全能力技术要求》

3 术语、定义和缩略语

3.1 术语和定义

下列术语和定义适用于本文件。

3.1.1 移动智能终端

能够接入移动通信网，具有能够提供应用软件开发接口的开放操作系统，具有安装、加载和运行应用软件能力的终端。

3.1.2 移动智能终端应用软件

移动智能终端内，能够利用移动智能终端操作系统提供的开发接口，实现某项或某几项特定任务的计算机软件或者代码片段。包含移动智能终端预置应用软件，以及互联网信息服务提供者提供的可以通过网站、应用商店等移动应用分发平台下载、安装、升级的应用软件。

3.1.3 移动智能终端操作系统

移动智能终端最基本的系统软件，它控制和管理移动智能终端各种硬件和软件资源，并提供应用程序开发接口。

3.1.4 移动应用分发平台

移动应用分发平台（以下简称“分发平台”）是指网站、移动应用分发软件等提供移动智能终端应

用软件下载、安装、升级的应用软件平台。

3.1.5 移动智能终端预置应用软件

移动智能终端内，在主屏幕和辅助屏界面（不包含进入界面后，通过菜单进入或者调起的功能）有用户交互入口并且可独立使用的移动智能终端应用软件。

3.1.6 用户

使用移动智能终端资源的对象，包括人或第三方应用程序。

3.1.7 个人信息

以电子或者其他方式记录的能够单独或者与其他信息结合识别特定自然人身份或者反映特定自然人活动情况的各种信息。

3.1.8 敏感个人信息

一旦泄露、非法提供或滥用可能危害人身和财产安全，极易导致个人名誉、身心健康受到损害或歧视性待遇等的个人信息。

3.1.9 个人信息主体

个人信息所标识或者关联的自然人。

3.1.10 个人信息控制者

有能力决定个人信息处理目的、方式等的组织或个人。

3.1.11 明示同意

个人信息主体通过书面、口头等方式主动作出纸质或电子形式的声明，或者自主作出肯定性动作，对其个人信息进行特定处理作出明确授权的行为。

3.1.12 用户画像

通过收集、汇聚、分析个人信息，对某特定自然人个人特征，如职业、经济、健康、教育、个人喜好、信用、行为等方面作出分析或预测，形成其个人特征模型的过程。

3.1.13 共享

个人信息控制者向其他控制者提供个人信息，且双方分别对个人信息拥有独立控制权的过程。

3.1.14 关联

通过唯一识别标识，将不同机构、终端、应用收集到的信息进行匹配、整合。

3.1.15 公开披露

向社会或不特定人群发布信息的行为。

3.1.16 终端告知

终端(终端厂商、终端操作系统或终端预置应用)通过各种方式告知用户，将对其个人信息进行特定处理的行为。

3.1.17 终端告知同意

终端(终端厂商、终端操作系统或终端预置应用)通过各种方式告知用户，并获得用户明确授权对其个人信息进行特定处理的行为。

3.1.18 应用软件告知同意

移动终端上的应用软件通过弹窗或产品界面等方式提示用户收集使用相关权限或信息的目的、方式、范围等，并获用户做出明确授权的行为。

3.1.19 收集

获得个人信息的控制权的行为，包括由个人信息主体主动提供、通过与个人信息主体交互或记录个人信息主体行为等自动采集行为，以及通过共享、转让、搜集公开信息等间接获取个人信息等行为。

注：如果产品或服务的提供者提供工具供个人信息主体使用，提供者不对个人信息进行访问的，则不属于本标准所称的收集。例如，离线导航软件在终端获取用户位置信息后，如果不回传至软件提供者，则不属于用户位置信息的收集。

3.1.20 采集

产品或服务获取的个人信息存储在个人信息主体本地设备内，供个人信息主体本地操作，不上传至软件提供者的行为。

3.1.21 使用

对个人信息进行加工、处理的过程。

3.1.22 敏感权限

敏感权限对应的数据或资源，涉及下列范围：个人信息或个人敏感信息，一旦泄露、非法提供或滥用可能危害人身和财产安全；对用户存储的数据或其他应用的操作产生影响，可能干扰系统正常运行或实施恶意行为。

4 个人信息保护原则

参考GB/T35273-2020 《个人信息安全规范》，个人信息保护应遵循以下基本原则：

权责一致、目的明确、选择同意、最小必要、公开透明、确保安全、主体参与。

5 移动终端个人信息服务分类及管理要求

移动终端上的应用软件和操作系统服务均涉及个人信息处理。移动终端上的应用软件按照在移动终端上的部署形式，分为预置应用软件、用户自主安装的三方应用软件，其中预置应用软件包括移动终端预置的应用软件、三方应用预置在移动终端的应用软件。操作系统服务包括有交互入口的操作系统服务、没有用户交互入口的操作系统服务。

三方应用软件的个人信息处理应符合国家、行业法律法规等要求。

终端上的预置应用软件、操作系统服务的个人信息处理应符合YD/T 2407-XXXX 《移动智能终端安全能力技术要求》中个人信息处理的要求，并至少满足1级要求。

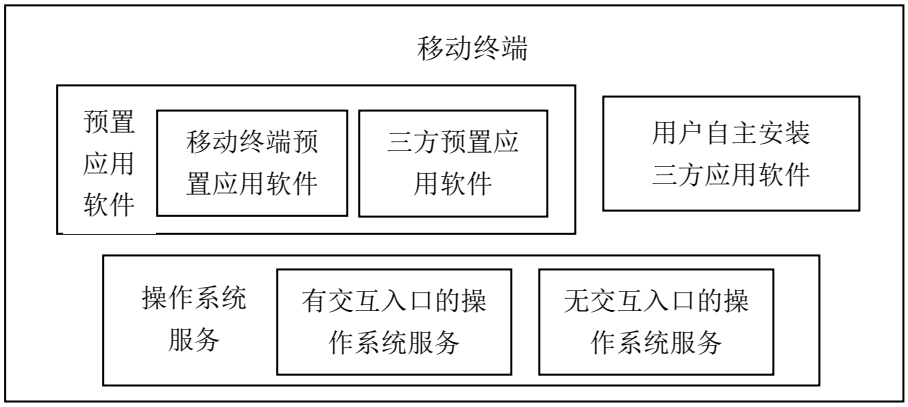

图1 移动终端个人信息服务分类图

6 移动终端和应用软件用户个人信息生命周期

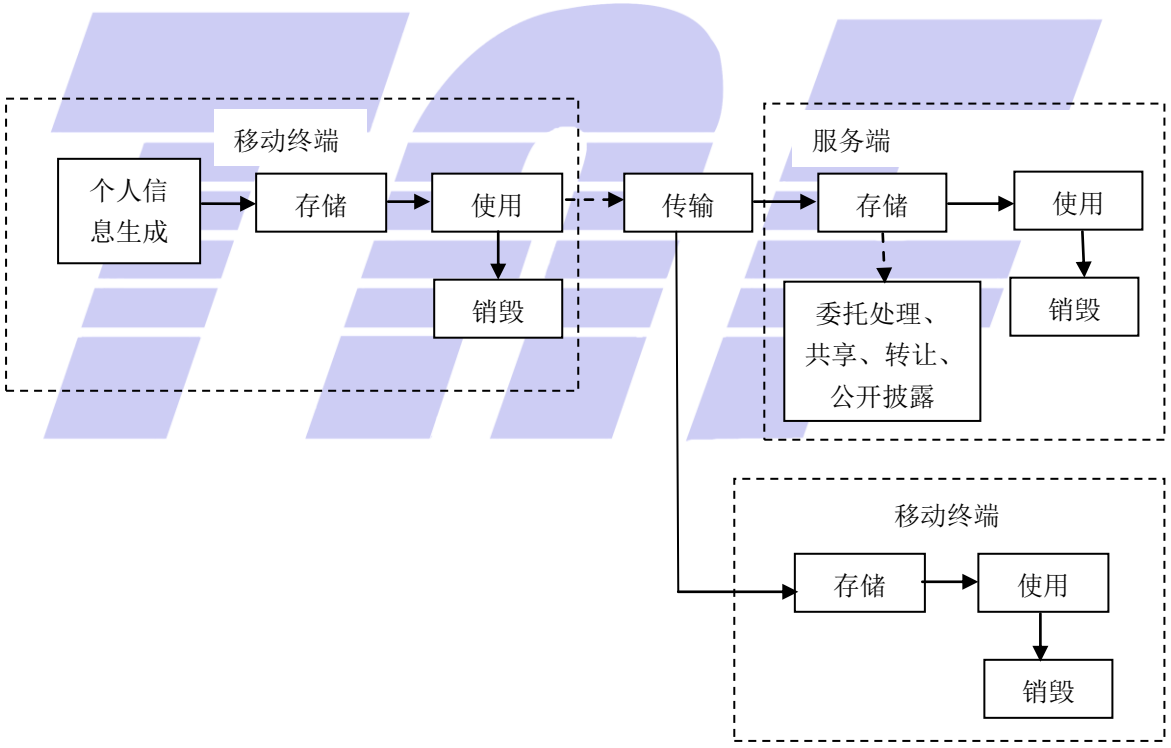

图2 移动终端和应用软件用户个人信息生命周期

个人信息生成：

移动终端和其上的应用软件通过收集、直接生成、或其他方式转入产生用户个人信息的过程。

存储：

用户个人信息在移动终端或服务器端上存留的过程。

使用：

用户个人信息在移动终端或在服务器端被使用的过程。

销毁：

用户个人信息在终端或服务器端被删除的过程，保证其不可被检索、访问的状态。

传输：

指用户个人信息离开移动终端的过程。

个人信息流转：

指用户个人信息在服务端通过委托处理、共享、转让、公开披露等方式对个人信息操作的过程。

7 移动终端和应用软件用户个人信息生命周期安全要求

7.1 用户个人信息在移动终端上的生命周期安全要求

用户个人信息在移动终端上的生命周期包括个人信息生成、存储、使用、销毁，其各阶段的基本要求如下，具体要求参考本系列中其它分册的相应要求：

注：本系列中其它标准列表见附录A。

个人信息生成阶段：

移动终端和应用软件收集用户个人信息前应满足告知同意等合规性要求。

存储阶段：

为用户个人信息提供安全的存储环境，防止用户个人信息被窃取、篡改等操作。

移动终端上个人信息宜做分类分级处理，根据个人信息的使用场景进行分类，并根据个人信息的敏感程度、泄露和滥用对用户、系统等造成的影响程度划分敏感等级。

使用阶段：

移动终端及其上应用软件应合理申请使用权限。

为用户个人信息提供访问控制机制。

移动终端及其上应用软件应合理利用个人信息进行广告、个性化推送等行为。

销毁阶段：

移动终端及其上应用软件应为用户提供删除个人信息的途径。

移动终端及其上应用软件为用户提供账号注册服务，应提供注销账号的途径，并满足注销账号的要求。

7.2 用户个人信息传输过程安全要求

用户个人信息在传输过程中应保证个人信息的安全性，防止被监听、篡改。

离开移动终端的用户个人信息宜具备相同安全保护程度的保护和访问控制机制。

附录 A

（资料性附录）

下表为本系列其它标准：

标准名称
移动智能终端及应用软件用户个人信息保护实施指南 第2部分 个人信息分类分级
移动智能终端及应用软件用户个人信息保护实施指南 第3部分 终端告知同意
移动智能终端及应用软件用户个人信息保护实施指南 第4部分 应用软件告知同意
移动智能终端及应用软件用户个人信息保护实施指南 第5部分 终端权限管理
移动智能终端及应用软件用户个人信息保护实施指南 第6部分 应用软件敏感权限规范
移动智能终端与应用软件用户个人信息保护实施指南 第7部分 定向推送
移动智能终端及应用软件用户个人信息保护实施指南 第8部分 个人信息收集使用规则
移动智能终端与应用软件用户个人信息保护实施指南 第9部分 注销账户

终端产业协会团体标准

移动智能终端与应用软件用户个人信息保护实施指南 第 1 部分：总则

T/TAF XXX—XXXX

*

电信终端产业协会印发
地址：北京市西城区新街口外大街 28 号
电话：010-82052809
电子版发行网址：www.taf.org.cn