ICS 33.050
CCS M 30

团 体 标 准

T/TAF 161—2023

移动智能终端个人信息保护规范

Specification for personal information protection of smart mobile phone

2023-04-26 发布　　2023-04-26 实施

电信终端产业协会 发布

目　　次

前　言

本文件按照GB/T 1.1—2020《标准化工作导则　第1部分：标准化文件的结构和起草规则》的规定起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由电信终端产业协会提出并归口。

本文件起草单位：中国信息通信研究院、泰尔认证中心有限公司、华为终端有限公司、OPPO广东移动通信有限公司、荣耀终端有限公司、北京三星通信技术研究有限公司、维沃移动通信有限公司、博鼎实华（北京）技术有限公司、郑州信大捷安信息技术股份有限公司、蚂蚁科技集团股份有限公司。

本文件主要起草人：王淞鹤、宁华、宋恺、刘陶、傅山、王艳红、武林娜、王宇晓、邓佑军、王嘉义、杨萌科、杜云、周飞、李京典、陈鑫爱、李可心、汪海、魏凡星、王浩仟、桑明臣、张静怡、常琳、钱康、凌大兵、衣强、李腾、赵晓娜、蒲兴、王海峰、吴越、张玮、董雾、刘献伦、刘为华、林冠辰、石玉珍。

引　　言

近年来，随着我国移动互联网行业迅猛发展，移动智能终端类型和应用场景不断丰富，智能终端上的个人信息也面临着新的安全威胁。为了移动智能终端产业的健康持续发展，进一步提升终端上的个人信息保护能力，本文件根据《中华人民共和国个人信息保护法》等法律要求，依据《工业和信息化部关于开展纵深推进APP侵害用户权益专项整治行动的通知》对移动智能终端个人信息保护提出相应规范。

移动智能终端个人信息保护规范

1 范围

本文件规定了移动智能终端的个人信息保护要求与相应测评方法，从个人信息全生命周期保护、安全能力方面对移动智能终端及终端预置应用软件提出具体的规范要求并进行个人信息保护能力分级。

本文件适用于移动智能终端及终端预置应用软件，其他类型的终端可参考使用。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 34978—2017 信息安全技术 移动智能终端个人信息保护技术要求

GB/T 41391—2022 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

YD/T 2407—2021 移动智能终端安全能力技术要求

YD/T 2408—2021 移动智能终端安全能力测试方法

3 术语和定义

下列术语和定义适用于本文件。

3.1

用户 user

使用移动智能终端资源或移动互联网应用程序的个人信息主体。

3.2

移动智能终端 smart mobile terminal

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

3.3

移动智能终端操作系统 operating system of smart mobile terminal

运行在移动智能终端上的系统软件，控制、管理移动智能终端上的硬件和软件，提供用户操作界面、应用软件编程接口和其他系统服务的应用软件。

3.4

移动智能终端应用软件　smart mobile terminal application

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。

3.5

移动智能终端预置应用软件　smart mobile terminal pre—installed application

由移动智能终端生产企业预置，在移动智能终端主屏幕或辅助屏幕界面（不包含进入界面后，通过菜单进入或者调起的功能）内存在用户交互入口，为满足用户不同的应用需求而提供的、可独立使用的软件程序。

注：通常简称预置应用。

3.6

明示同意　expressed consent

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。

3.7

个人信息　personal information

以电子或者其他方式记录的与已识别或可识别的自然人有关的各种信息,不包括匿名化处理后的信息。

[来源：《中华人民共和国个人信息保护法》]

3.8

敏感个人信息　sensitive personal information

一旦泄露或者非法使用,可能导致自然人的人格尊严受到侵害或者人身、财产安全受到危害的个人信息,包括生物识别、宗教信仰、特定身份、医疗健康、金融账户、行踪轨迹等信息，以及不满十四周岁未成年人的个人信息。

[来源：《中华人民共和国个人信息保护法》]

3.9

删除　delete

在实现日常业务功能所涉及的系统中去除个人信息的行为，使其保持不可被检索、访问的状态。

[来源：GB/T 35273—2020,3.10]

3.10

匿名化 anonymization

通过对个人信息的技术处理，使得个人信息主体无法被识别或者关联，且处理后的信息不能被复原的过程。

3.11

去标识化 de—identification

通过对个人信息的技术处理，使其在不借助额外信息的情况下，无法识别或者关联个人信息主体的过程。

[来源：《中华人民共和国个人信息保护法》]

3.12

收集 collect

获取个人信息的活动。

3.13

匿名设备识别码 anonymous device identity

用于短期内标识终端设备的数据信息，可根据需要进行改变。

4 缩略语

下列缩略语适用于本文件。

IMEI：国际移动设备识别码（International Mobile Equipment Identity）
MAC：媒体存取控制位址（Media Access Control）
OAID：匿名设备标识符（Open Anonymous Device Identifier）

5 移动智能终端个人信息保护目标

5.1 个人信息全生命周期保护目标

移动智能终端自身及预置应用软件在提供相关服务或实现相关功能时收集个人信息应遵循最小必要原则，同时在个人信息处理过程中，应确保个人信息存储、使用、传输环节的安全，以及为个人信息的查询、更正与删除等个人信息主体权利的行使提供相应保证。

5.2 个人信息安全能力目标

移动智能终端通过对系统资源调度的监控、保护、提醒及对移动应用访问终端上的特定个人信息等相关行为的安全性控制，使得涉及个人信息的移动应用行为及系统行为总是在受控状态下，确保不会出现损害个人信息安全权益的行为。

6 个人信息全生命周期保护要求

6.1 个人信息的收集

6.1.1 收集个人信息的授权同意

6.1.1.1 收集个人信息的告知

移动智能终端及预置应用软件应通过以下方式对用户进行收集个人信息的告知：

a） 收集个人信息前，应通过隐私政策或其他显著告知方式向用户告知收集个人信息的类型、使用目的和方式。告知场景包括：
   1） 用户首次启动或是恢复出厂设置等初始化移动智能终端；
   2） 用户首次启动预置应用软件；
   3） 用户首次使用涉及收集个人信息的功能服务时。

b） 当收集个人信息的种类、处理目的、处理方式、保存期限等发生重大变更时，应当重新告知用户；

c） 告知内容涉及用户敏感个人信息的，应通过明确标识或突出显示等方式标注处理敏感个人信息相关的告知内容，以提醒个人予以重点关注；

d） 收集敏感个人信息前，应通过设置专门页面或单独步骤等方式向用户增强告知收集敏感个人信息的类型、处理目的、处理方式，确保用户充分了解处理敏感个人信息的目的；

e） 收集不满十四周岁未成年人个人信息的，应制定专门的个人信息处理规则并告知未成年人的父母或监护人。

6.1.1.2 收集个人信息的同意

移动智能终端及预置应用软件基于个人同意收集个人信息的，应满足以下条件：

a） 收集个人信息前，应获得用户的授权同意；

b） 在告知用户并需要获得授权同意时，应当为用户提供可采取同意和拒绝的选项，或由用户自主作出肯定性动作进行同意；

c） 当收集个人信息的种类、处理目的、处理方式、保存期限等发生重大变更时，应重新征得用户的授权同意。

注：肯定性动作包括个人主动勾选、主动点击“同意”“注册”“发送”“拨打”、主动填写或提供等。

6.1.1.3 收集敏感个人信息的单独同意

移动智能终端及预置应用收集敏感个人信息的，应满足以下要求：

a） 收集敏感个人信息前，应征得用户的单独同意；

b） 收集不满 14 周岁未成年人个人信息的，应当取得未成年人的父母或其他监护人的同意。

6.1.1.4 基于个人信息访问控制能力的告知与授权

涉及通过系统弹窗申请个人信息访问控制能力的，预置应用软件应满足以下要求：

a） 获取个人信息访问控制能力前，应向用户告知获取的目的；

b） 不应强制、频繁、过度索取个人信息访问控制能力。

注 1：个人信息访问控制能力指对终端所具有的且可提供给应用软件使用的个人信息的读取、写入、删除等能力，在安卓系统中个人信息访问控制能力可对应为安卓权限管控机制。

注 2：强制、频繁、过度索取行为描述见 YD/T 4184—2022《移动互联网应用程序（APP）用户权益保护测评规范》。

6.1.1.5 操作系统敏感行为的告知与授权

移动智能终端操作系统敏感行为的告知与授权，具体应符合 YD/T 2407—2021 5.3.5.2 规定的相关要求。

6.1.2 收集个人信息的最小必要

移动智能终端及预置应用软件收集个人信息的类型应当具有明确、合理的目的，并应当限于实现其收集目的的最小范围，不得进行与其目的无关的个人信息收集。

6.1.3 个人信息的主动提供

移动智能终端及预置应用软件不应在非服务或无合理场景，在信息窗口页面通过积分、奖励、优惠等方式欺骗误导用户提供身份证号、人脸、指纹等个人信息。

6.2 个人信息的存储

6.2.1 个人信息的保存期限

移动智能终端及预置应用软件保存个人信息的期限，应满足以下要求：

a） 为实现用户授权使用的目的所必需的最短时间，法律法规另有规定或者用户另行授权同意的除外；

b） 对超出保存期限的敏感个人信息进行删除或匿名化处理。

注：对于用户保存在端侧的个人信息，移动智能终端及预置应用软件只需对业务运行过程中产生的包含个人信息的缓存文件，或过程文件自行决定删除时间，其它个人信息由用户自己管理和控制。

6.2.2 个人信息的本地存储

移动智能终端及预置应用软件的本地化存储，应遵循以下要求：

a） 移动智能终端应提供对应用程序运行过程中产生且本地化存储的临时文件的访问控制机制；

b） 应根据个人信息的类别和级别实行不同安全级别的处理及保护方式（如加密存储等）；

c） 应对用户口令安全存储并进行安全访问控制；

d） 加密密钥应采用基于硬件的安全保护。

6.3 个人信息的使用

6.3.1 个人信息的安全性控制

在对个人信息的使用过程中，移动智能终端及预置应用软件应对个人信息访问进行安全性控制，保证个人信息的分析处理过程稳定安全地运行在安全沙箱等独立资源空间，不造成个人信息的损毁、泄露和丢失等。

6.3.2 个人信息的展示限制

涉及通过界面展示个人信息的（如显示屏幕中的弹框、通知、浮窗等），移动智能终端及预置应用软件应提供对展示中涉及的敏感个人信息采取屏蔽处理、隐藏通知内容等措施的能力，降低在账号登陆、消息通知、短信接收等敏感个人信息展示环节的泄露风险。

6.3.3 个性化推荐

移动智能终端及预置应用软件的个性化推荐，应遵循以下要求：

a) 在相应的业务功能界面中显著区分个性化推荐服务，如标明“推荐”或“猜你喜欢”等字样；
b) 应提供退出或关闭个性化推荐模式的选项，如拒绝接受定向推送信息，或停止、退出、关闭相应功能的机制。当用户退出或关闭个性化推荐模式并撤销相关个人信息的收集许可，应及时停止继续收集仅用于个性化推荐相关服务的个人信息；
c) 移动智能终端及预置应用软件提供个性化推荐服务，若因提供个性化推荐服务涉及向第三方提供个人信息的，应向用户明示并获得用户同意，法律法规规定的除外；
d) 向个人信息主体提供隐私保护相关投诉和反馈渠道，支持对个性化推荐服务问题的受理。

6.4 个人信息的加工

移动智能终端及预置应用软件加工个人信息应满足以下要求：

a) 加工个人信息的目的、方式、范围不应超出业务功能的实际需要或合理关联，法律法规另有规定的除外；
b) 直接获取或通过第三方间接获取个人信息，进行加工处理形成新的个人信息并用于其他目的，应告知用户，如以同意为合法基础的，应再次征得用户的同意；
c) 加工个人信息应保证加工过程可控、加工结果准确及完整，符合加工处理的预期。

6.5 个人信息的传输

移动智能终端及预置应用软件对个人信息的传输应满足如下要求：

a) 进行个人信息传输应按照约定目的和用途进行，传输数据之前应对数据接收方进行身份确认和授权；
b) 若通过公共网络传输账户设置、传感采集（包括个人健康生理信息、运动信息、位置信息等）、金融支付等服务相关的个人信息时，应保证数据的完整性和机密性。若涉及敏感个人信息传输的，应进行加密保护（例如HTTPS）。

6.6 个人信息的查询、更正与删除

6.6.1 个人信息的查询

移动智能终端及预置应用软件应向用户提供查询下列信息的方法：

a) 其所持有的关于该用户的个人信息，包括用户主动提供的、移动智能终端及预置应用软件提供相关服务时收集的个人信息；
b) 上述个人信息所用于的目的、范围；
c) 获得上述个人信息的第三方组织、身份或类型。

注：用户提出查询非其主动提供的个人信息时，可在综合考虑不响应请求可能对用户合法权益带来的风险和损害，以及技术可行性、实现请求的成本等因素后，作出是否响应的决定，并给出解释说明。

6.6.2 个人信息的更正

用户发现其个人信息有错误或不完整的，移动智能终端及预置应用软件应为其提供请求更正或补充信息的方法。

6.6.3 个人信息的删除

移动智能终端及预置应用软件应满足以下个人信息删除要求：

a） 应清楚告知用户，可删除个人信息的方法或途径；

b） 对个人信息本地存储操作，应提供个人信息彻底删除能力，以保证被删除的个人信息不可恢复；

c） 在以下情形中，移动智能终端及预置应用软件应主动删除个人信息，移动智能终端及预置应用软件未删除的，个人有权请求删除：

1） 个人信息处理目的已实现、无法实现或者为实现处理目的不再必要；

2） 停止提供产品或服务，或者保存期限已届满；

3） 个人撤回同意；

4） 违反法律法规或者违反约定处理个人信息；

5） 法律法规所规定的其他情形。

d） 法律、行政法规规定的保存期限未届满，或者删除个人信息从技术上难以实现的，移动智能终端及预置应用软件应当停止除存储和采取必要的安全保护措施之外的处理。

7 个人信息安全能力要求

7.1 个人信息数据访问控制管理

7.1.1 个人信息访问控制能力

根据获取对应个人信息数据访问控制能力后对用户、操作系统造成的风险程度，个人信息访问控制可分为一般的个人信息访问控制和敏感的个人信息访问控制。 按照不同的保护等级要求，移动终端操作系统可以提醒用户授权，或者自动授予应用相关数据访问控制能力。

a） 一般的个人信息访问控制涉及对用户私有数据或资源的访问控制，如粗略位置信息、应用软件安装列表等。应用软件申请对该类个人信息的访问控制时，移动智能终端应保证该应用软件在获得对应访问控制能力前，无法对相关数据进行访问控制；

注：应用软件获得一般个人信息访问控制能力可通过应用声明或者用户对相应弹窗授权做出同意来实现。

b） 敏感的个人信息访问控制涉及对与用户具有强关联性且对用户隐私安全影响较大的敏感数据或资源的访问控制，包括精确地理位置、多媒体信息（如照片、语音、视频信息）等。移动智能终端在应用软件申请敏感个人信息访问控制时，以系统弹窗等形式向用户明示并申请授权。在用户授权之前，移动智能终端应确保应用软件无法对相关数据进行访问控制。

7.1.2 个人信息访问控制管理机制

移动智能终端对个人信息访问控制能力的申请、授予、撤销、升级和配置管理要求如下：

a） 申请要求：应提供访问控制能力显性告知的提示方式，方式可以为弹框、通知、浮窗等，在移动应用软件向移动智能终端申请获取个人信息的访问控制能力时，移动智能终端应在用户主动确认同意授予后执行相应操作；

b） 授予要求：访问控制能力的授予可根据具体场景分为允许、禁止、询问等选项供用户自由选择；

c） 撤销要求：应提供对已授予的个人信息访问控制能力撤销授予的功能，用户可在相关管理界面针对单独应用软件进行相关数据的访问控制能力的撤销授予操作，可修改为禁止或询问；

d） 配置管理要求：应提供个人信息访问控制能力配置管理功能，供用户自主选择（如应用软件维度及个人信息访问控制维度）。用户可在相关配置管理界面对移动应用软件的个人信息访问控制能力进行授予、撤销等操作；

e） 一致性要求：已授予的个人信息访问控制能力在移动智能终端操作系统或应用软件版本升级前后应保持一致，如出现能力变更等变化情况，应向用户明示并征得用户授权同意。

7.1.3 安全调用控制能力

移动智能终端应对本地功能进行安全调用控制，具体应满足以下要求:

a） 通信类功能受控机制应符合 YD/T 2407—2021 5.3.1.1 规定的相关要求；

b） 本地敏感功能受控机制应符合 YD/T 2407—2021 5.3.1.2 规定的相关要求。

7.2 敏感行为管理

7.2.1 应用软件行为记录能力要求

移动智能终端应支持并统计应用软件调用行为，且用户可查看记录结果，具体应符合如下要求：

a） 应符合 YD/T 2407—2021 5.5.2a）的相关要求；

b） 应符合 YD/T 2407—2021 5.5.2b）的相关要求；

c） 移动智能终端对自研预置应用软件的行为记录应参照本节 a）执行；

d） 移动智能终端对自研预置应用软件的行为记录应参照本节 b）执行。

7.2.2 行为记录安全管理要求

为保证调用行为记录的完整性、真实性和有效性，移动智能终端应满足如下要求：

a） 应保证调用行为记录的准确性，具体包括：

1） 移动智能终端操作系统对调用行为的记录应在应用软件调用相应功能接口后开始记录，调用行为的起始时间为应用软件调用相应功能接口的时间；

2） 移动智能终端操作系统对调用行为的记录应在行为发生起始时间 1 分钟内生成，确保记录内容的准确性，不应出现记录内容缺失、错误现象。

b） 应提供调用行为记录数据保护机制，防止调用行为记录数据库被恶意删改。

7.2.3 应用软件敏感行为状态展示

移动智能终端应提供应用软件敏感行为状态展示功能，当移动终端应用软件存在调用定位服务、麦克风、摄像头等行为时，应通过持续性状态指示等显著方式对用户进行敏感行为展示。

7.2.4 高风险行为监测

移动智能终端应对 APP 静默安装、热更新等高风险行为进行监测，包括但不限于以下行为：

a） 未经用户同意私自安装APP；

b） 通过热更新的方式非法改变APP功能、APP图标；

7.3 匿名设备识别码

当移动智能终端提供匿名设备识别码时应满足以下要求：

a） 匿名设备识别码的生成应具备不可逆性，仅由匿名设备识别码无法关联到该设备的其他非匿名设备识别码；

b） 应向用户提供重置匿名设备识别码的方法。

c） 应为用户提供关闭匿名设备识别码的机制，用户关闭后，APP调用时终端不应返回匿名设备识别码，应返回0或返回关闭状态值，确保应用软件无法使用匿名设备识别码识别到终端设备。

注：匿名设备识别码指 OAID 等可变识别码。

7.4 自启动与关联启动行为管理

移动智能终端应提供对应用软件自启动与关联启动行为的管理功能，应满足以下要求：

a） 提供应用软件自启动、关联启动关闭选项；

b） 提供应用软件自启动、关联启动行为记录，包括自启动、关联启动的时间或启动次数，以及关联启动源、目的应用软件等信息。

c） 提供应用软件关联启动实时提示功能。

7.5 系统更新安全管理

移动智能终端应提供操作系统更新安全管理能力，提供操作系统的更新机制（包含系统、驱动和系统服务的安装更新）时，应在执行更新安装操作前提示用户，并在用户确认后执行相关操作。

7.6 APP 下载、使用、安装管理

移动智能终端及预置应用软件向用户提供 APP 下载、安装、使用的功能或服务时，应满足以下要求：

a） 应以显著方式向用户明示、并征得用户主动选择同意，不应在用户点击信息窗口任意位置即下载、安装、使用APP。

b） 不应欺骗误导用户下载、安装、使用APP，包括但不限于在未明示下载APP情况下通过在信息窗口展示“是否立即开始游戏”、“领取红包”、“手机卡顿”、“耗电太快”、“内存已满”等信息诱导用户点击并下载安装。

c） 用户暂停或取消的APP下载、安装服务后，不应自动恢复下载、安装。

d） 信息窗口中展示的APP信息应与实际下载、安装的APP信息相符。

8 测试方法

8.1 个人信息保护测评

8.1.1 个人信息的收集

8.1.1.1 收集个人信息的告知

8.1.1.1.1 测评项:详见6.1.1.1a)

根据具体检测场景需求,可选用8.1.1.1.2、8.1.1.1.3、8.1.1.1.4三种测试方法。

8.1.1.1.2 测评项：详见6.1.1.1a)的1)

该项测评方法如下：

a) 指标要求：移动智能终端应对用户进行收集个人信息的告知；
b) 测评对象：移动智能终端；
c) 测评方式：功能验证、技术检测；
d) 预置条件：
   1) 被测移动智能终端处于正常工作状态；
   2) 被测移动智能终端打开测试模式。
e) 测评步骤：
   1) 初始化移动智能终端或是恢复出厂设置，判断其是否存在个人信息收集行为；
   2) 使用检测工具监测移动智能终端个人信息收集行为,判断其收集个人信息前是否通过隐私政策或其他显著告知方式向用户告知收集个人信息的类型和使用目的。
f) 单元判定：如果1）、2）结果均为肯定，则测试项判定为未见异常，否则判定为不符合要求。

8.1.1.1.3 测评项：详见6.1.1.1a)的2)

该项测评方法如下：

a) 指标要求：预置应用软件启动时个人信息的告知；
b) 测评对象：预置应用软件；
c) 测评方式：功能验证、技术检测；
d) 预置条件：
   1) 被测预置应用软件处于正常工作状态；
   2) 移动智能终端打开测试模式。
e) 测评步骤：
   1) 使用检测工具监测预置应用软件的初始化,判断其启动是否通过隐私政策或其他显著告知方式向用户告知其个人信息行为；
   2) 查看预置应用软件告知声明，判断其告知内容是否包含收集个人信息的类型、使用目的及处理规则。
f) 单元判定：如果1）、2）结果均为肯定，则测试项判定为未见异常，否则判定为不符合要求。

8.1.1.1.4 测评项：详见6.1.1.1a)的3)

该项测评方法如下：

a) 指标要求：首次使用涉及收集个人信息的功能服务时的告知；
b) 测评对象：移动智能终端、预置应用软件；
c) 测评方式：功能验证、技术检测；

d） 预置条件：

1） 被测移动智能终端和预置应用软件处于正常工作状态；

2） 移动智能终端打开测试模式。

e） 测评步骤：

1） 使用检测工具监测移动智能终端和预置应用软件，判断其在用户首次使用涉及收集个人信息前是否通过隐私政策或其他显著告知方式告知用户。

f） 单元判定：如果1）结果均为肯定，则测试项判定为未见异常，否则判定为不符合要求。

8.1.1.1.5 测评项：详见6.1.1.1b）

该项测评方法如下：

a） 指标要求：移动智能终端及预置应用软件收集个人信息发生重大变更时的告知；

b） 测评对象：移动智能终端、预置应用软件；

c） 测评方式：功能验证、技术检测；

d） 预置条件：

1） 被测移动智能终端及预置应用软件处于正常工作状态；

2） 被测移动智能终端打开测试模式。

e） 测评步骤：

1） 使用检测工具监测移动智能终端及预置应用软件，判断当收集个人信息的种类、处理目的、处理方式、保存期限等发生重大变更时，是否重新告知用户。

f） 单元判定：如果1）结果均为肯定，则测试项判定为未见异常，否则判定为不符合要求。

8.1.1.1.6 测评项：详见6.1.1.1c）

该项测评方法如下：

a） 指标要求：移动智能终端及预置应用软件应通过明确标识或突出显示等方式标注处理敏感个人信息相关的告知内容；

b） 测评对象：移动智能终端、预置应用软件；

c） 测评方式：功能验证；

d） 预置条件：

1） 被测移动智能终端及预置应用软件处于正常工作状态；

2） 被测移动智能终端打开测试模式。

e） 测评步骤：

1） 监测移动智能终端及预置应用软件，判断其向用户告知收集敏感个人信息时是否通过明确标识或突出显示等方式标注处理敏感个人信息相关的告知内容。

f） 单元判定：如果1）结果均为肯定，则测试项判定为未见异常，否则判定为不符合要求。

8.1.1.1.7 测评项：详见6.1.1.1d）

该项测评方法如下：

a） 指标要求：移动智能终端及预置应用软件收集敏感个人信息的告知；

b） 测评对象：移动智能终端、预置应用软件；

c） 测评方式：功能验证、技术检测；

d） 预置条件：

1） 被测移动智能终端及预置应用软件处于正常工作状态；

2） 被测移动智能终端打开测试模式。

e） 测评步骤：

1） 判断移动智能终端及预置应用软件是否涉及收集敏感个人信息；

2） 检测移动智能终端及预置应用软件，判断其是否在收集敏感个人信息前，通过设置专门页面或单独步骤等方式向用户增强告知收集敏感个人信息的类型、处理目的、处理方式。

f） 单元判定：如果1）结果为否定，则测试项判定为不适用；如果1）、2）结果均为肯定，则测试项判定为未见异常，否则判定为不符合要求。

8.1.1.1.8 测评项：详见6.1.1.1e）

该项测评方法如下：

a） 指标要求：移动智能终端及预置应用软件涉及收集不满十四周岁未成年人个人信息的告知；

b） 测评对象：移动智能终端、预置应用软件；

c） 测评方式：功能验证、技术检测；

d） 预置条件：

1） 被测移动智能终端及预置应用软件处于正常工作状态；

2） 被测移动智能终端打开测试模式。

e） 测评步骤：

1） 判断移动智能终端及预置应用软件是否涉及收集不满十四周岁未成年人个人信息；

2） 检测移动智能终端及预置应用软件，判断其是否针对不满十四周岁未成年人制定专门的个人信息处理规则。

f） 单元判定：如果1）结果为否定，则测试项判定为不适用；如果1）、2）结果均为肯定，则测试项判定为未见异常，否则判定为不符合要求。

8.1.1.2 收集个人信息的同意

8.1.1.2.1 测评项：详见6.1.1.2

该项测评方法如下：

a） 指标要求：移动智能终端及预置应用软件基于个人同意收集个人信息的，应获得用户的授权同意。在告知用户并需要获得授权同意时，应当为用户提供可采取同意或拒绝的选项，通过用户对信息收集主动作出肯定性动作征得用户明示同意，当收集个人信息的种类、处理目的、处理方式、保存期限等发生重大变更时，应重新征得用户的明示同意；

b） 测评对象：移动智能终端、预置应用软件；

c） 测评方式：功能验证、技术检测；

d） 预置条件：

1） 被测移动智能终端及预置应用软件处于正常工作状态；

2） 被测移动智能终端打开测试模式。

e） 测评步骤：

1） 使用检测工具监测移动智能终端或预置应用软件，判断其收集个人信息，是否获得用户的授权同意；

2） 查看移动智能终端或预置应用软件是否为用户提供可采取同意或拒绝的选项，并通过用户对信息收集主动作出肯定性动作征得用户明示同意；

3） 查看当收集个人信息的种类、处理目的、处理方式、保存期限等发生重大变更时，是否重新征得用户的明示同意。

f） 单元判定：如果1）、2）、3）结果为肯定，则测试项判定为未见异常，否则判定为不符合要求。

8.1.1.3 收集敏感个人信息的单独同意

8.1.1.3.1 测评项：详见6.1.1.3a）

该项测评方法如下：

a） 指标要求：移动智能终端及预置应用收集敏感个人信息，应征求并获得用户的单独同意；

b） 测评对象：移动智能终端、预置应用软件；

c） 测评方式：功能验证、技术检测；

d） 预置条件：

1） 被测移动智能终端及预置应用软件处于正常工作状态；

2） 被测移动智能终端打开测试模式。

e） 测评步骤：

1） 使用检测工具监测移动智能终端或预置应用软件，判断其收集敏感个人信息，是否征得用户单独同意。

f） 单元判定：如果1）结果为肯定，则测试项判定为未见异常，否则判定为不符合要求。

8.1.1.3.2 测评项：详见6.1.1.3b）

该项测评方法如下：

a） 指标要求：移动智能终端及预置应用收集不满14周岁未成年人个人信息的，应征求并获得未成年人的父母或其他监护人的同意。；

b） 测评对象：移动智能终端、预置应用软件；

c） 测评方式：功能验证、技术检测；

d） 预置条件：

1） 被测移动智能终端及预置应用软件处于正常工作状态；

2） 被测移动智能终端打开测试模式。

e） 测评步骤：

1） 使用检测工具监测移动智能终端或预置应用软件，判断其收集不满十四周岁未成年人的个人信息时是否征得未成年人的父母或其他监护人的同意。

f） 单元判定：如果1）结果为肯定，则测试项判定为未见异常，否则判定为不符合要求。

8.1.1.4 基于个人信息访问控制能力的告知和授权

8.1.1.4.1 测评项：详见6.1.1.4a）

该项测评方法如下：

a） 指标要求：涉及通过系统弹窗申请个人信息访问控制能力的，预置应用软件获取可收集个人信息相关数据的访问能控制能力前，应向用户告知获取的目的，并征得用户的明示同意；

b） 测评对象：预置应用软件；

c） 测评方式：功能验证、技术检测；

d） 预置条件：

1） 被测预置应用软件处于正常工作状态；

2） 移动智能终端打开测试模式。

e） 测评步骤：

1） 使用检测工具监测预置应用软件，判断其是否涉及通过系统弹窗申请个人信息访问控制能力；

2） 判断预置应用软件获取个人信息访问能控制能力前，是否向用户告知获取的目的，并征得用户的明示同意。

f） 单元判定：如果1）结果为否定，则测试项判定为不适用；如果2）结果为肯定，则测试项判定为未见异常，否则判定为不符合要求。

8.1.1.4.2 测评项：详见6.1.1.4b）

该项测评方法如下：

a） 指标要求：不应强制、频繁、过度索取个人信息访问控制能力；

b） 测评对象：预置应用软件；

c） 测评方式：功能验证、技术检测；

d） 预置条件：

1） 被测预置应用软件处于正常工作状态；

2） 移动智能终端打开测试模式。

e） 测评步骤：

1） 查看移动智能终端预置应用软件在用户拒绝授予个人信息访问控制能力时，预置应用软件是否退出或关闭，拒绝注册或登录，或拒绝提供与申请权限无关的功能服务；

2） 查看移动智能终端预置应用软件在用户拒绝授予个人信息访问控制能力时，预置应用软件是否循环弹窗；

3） 查看移动智能终端预置应用软件是否在未提供相关业务功能或服务时，申请无关个人信息访问控制能力的行为；

4） 查看移动智能终端预置应用软件是否在未见使用个人信息对应的相关业务功能或服务时，提前申请个人信息访问控制能力的行为；

5） 查看移动智能终端预置应用软件是否存在频繁申请个人信息访问控制能力的行为。

f） 单元判定：如果1）、2）、3）、4）、5）结果均为否定，则测试项判定为未见异常；否则判定为不符合要求。

注：电话、通讯录、短信、录音、相机、相册、日历等基本功能软件的基本功能所对应申请的权限除外。

8.1.1.5 操作系统敏感行为的告知与授权

8.1.1.5.1 测评项：详见6.1.1.5

该项测评方法如下：

a) 指标要求：见YD/T 2407—2021 5.3.5.2a）节；

b) 测评对象：移动智能终端；

c) 测评方式：功能验证、技术检测；

d) 预置条件：

1) 被测移动智能终端处于正常工作状态；

2) 被测移动智能终端打开测试模式。

e) 测评步骤：

1) 查看并使用检测工具监测移动智能终端，判断其操作系统（可安装的系统组件）是否存在未向用户明示且未经用户同意，开启通话录音、本地录音、后台截屏/录屏、拍照/摄像、接收短信和定位，采集和传送生物特征识别信息（如指纹识别、人脸识别等），读取和传送用户本机号码、电话本数据、通话记录、短信数据、上网记录、日程表数据、读取媒体影音数据（如照片、视频和音频），读取生物特征识别信息（指纹识别、人脸识别等）、读取设备唯一可识别信息（如不可重置的设备标识符）、应用软件列表的行为。

f) 单元判定：如果1）结果为否定，则测试项判定为未见异常；如果1）结果为肯定，判定为不符合要求。

8.1.1.5.2 测评项：详见6.1.1.5

该项测评方法如下：

a) 指标要求：见YD/T 2407—2021 5.3.5.2b）节；

b) 测评对象：移动智能终端；

c) 测评方式：功能验证、技术检测；

d) 预置条件：

1) 被测移动智能终端处于正常工作状态；

2) 被测移动智能终端打开测试模式。

e) 测评步骤：

1) 查看并使用检测工具监测移动智能终端，判断其操作系统（可安装的系统组件）是否存在未向用户明示且未经用户同意，擅自调用终端通信功能，包括在用户无确认情况下拨打电话、发送短信、发送彩信，通过移动通信网络数据连接、WLAN网络连接、无线外围接口传送数据，以及开启移动通信网络、WLAN和无线外围接口并传输数据的行为。

f) 单元判定：如果1）结果为否定，则测试项判定为未见异常；如果1）结果为肯定，判定为不符合要求。

8.1.1.6 收集个人信息的最小必要

8.1.1.6.1 测评项：详见6.1.2

该项测评方法如下：

a） 指标要求：移动智能终端及预置应用软件收集个人信息的最小必要；

b） 测评对象：移动智能终端、预置应用软件；

c） 测评方式：功能验证、技术检测；

d） 预置条件：

1） 被测移动智能终端及预置应用软件处于正常工作状态；

2） 被测移动智能终端打开测试模式。

e） 测评步骤：

1） 使用检测工具监控移动智能终端或预置应用软件，判断其是否存在个人信息收集行为；

2） 使用检测工具监测移动智能终端或预置应用软件，判断其收集个人信息是否具有明确、合理的目的，是否限于实现其收集目的的最小范围。

f） 单元判定：若1）为否定，则本测试项为不适用；如果1）、2）结果均为肯定，则测试项判定为未见异常，否则判定为不符合要求。

8.1.1.7 个人信息的主动提供

8.1.1.7.1 测评项：详见6.1.3

该项测评方法如下：

a） 指标要求：欺骗误导用户提供个人信息；

b） 测评对象：移动智能终端、预置应用软件；

c） 测评方式：功能验证、技术检测；

d） 预置条件：

1） 被测移动智能终端及预置应用软件处于正常工作状态；

2） 被测移动智能终端打开测试模式。

e） 测评步骤：

1） 判断移动智能终端及预置应用软件是否存在在APP信息窗口中通过积分、奖励、优惠等方式欺骗误导用户提供身份证号码、人脸、指纹等个人信息的行为。

f） 单元判定：如果1）结果为否定，则测试项判定为未见异常，否则判定为不符合要求。

8.1.2 个人信息的存储

8.1.2.1 个人信息的保存期限

8.1.2.1.1 测评项：详见6.2.1

该项测评方法如下：

a） 指标要求：移动智能终端及预置应用软件设置个人信息保存期限应为实现用户授权使用的目的所必需的最短时间，法律法规另有规定或者用户另行授权同意的除外；并对超出保存期限的敏感个人信息进行删除或匿名化处理；

b） 测评对象：移动智能终端、预置应用软件；

c） 测评方式：功能验证、技术检测；

d） 预置条件：

1） 被测移动智能终端及预置应用软件处于正常工作状态；
2） 被测移动智能终端打开测试模式。

e） 测评步骤：
1） 查阅移动智能终端或预置应用软件，判断其是否在隐私政策等文档中对个人信息保存期限进行声明；
2） 使用检测工具检测移动智能终端或预置应用软件，判断其是否对超出保存期限的敏感个人信息进行删除或匿名化处理。

f） 单元判定：如果1）、2）结果为肯定，则测试项判定为未见异常，否则判定为不符合要求。

8.1.2.2 个人信息的本地存储

8.1.2.2.1 测评项：详见6.2.2a）

该项测评方法如下：

a） 指标要求：移动智能终端应提供应用程序临时文件的访问控制；

b） 测评对象：移动智能终端、预置应用软件；

c） 测评方式：功能验证、技术检测；

d） 预置条件：
1） 被测移动智能终端及预置应用软件处于正常工作状态；
2） 被测移动智能终端打开测试模式。

e） 测评步骤：
1） 使用检测工具检测移动智能终端或预置应用软件，判断其是否提供应用程序临时文件的安全访问控制。

f） 单元判定：如果1）结果为肯定，则测试项判定为未见异常，否则判定为不符合要求。

8.1.2.2.2 测评项：详见6.2.2b）

该项测评方法如下：

a） 指标要求：移动智能终端及预置应用软件的本地化存储，应根据个人信息的类别和级别进行不同安全级别的处理及保护方式（如加密存储等）；

b） 测评对象：移动智能终端、预置应用软件；

c） 测评方式：功能验证、技术检测；

d） 预置条件：
1） 被测移动智能终端及预置应用软件处于正常工作状态；
2） 被测移动智能终端打开测试模式。

e） 测评步骤：
1） 使用检测工具查看移动智能终端及预置应用软件，判断其是否选择不同安全级别的加密手段对不同类别和级别的个人信息进行处理。

f） 单元判定：如果1）结果为肯定，则测试项判定为未见异常，否则判定为不符合要求。

8.1.2.2.3 测评项：详见6.2.2c）

该项测评方法如下：

a) 指标要求：移动智能终端及预置应用软件应对用户口令安全存储并进行安全访问控制；
b) 测评对象：移动智能终端、预置应用软件；
c) 测评方式：功能验证、技术检测；
d) 预置条件：
   1) 被测移动智能终端及预置应用软件处于正常工作状态；
   2) 被测移动智能终端打开测试模式。
e) 测评步骤：
   1) 使用检测工具查看移动智能终端及预置应用软件，判断其是否对用户口令安全存储并进行安全访问控制。
f) 单元判定：如果1）结果为肯定，则测试项判定为未见异常，否则判定为不符合要求。

8.1.2.2.4 测评项：详见6.2.2d）

该项测评方法如下：

a) 指标要求：加密密钥本地化存储，应采用基于硬件的安全保护；
b) 测评对象：移动智能终端；
c) 测评方式：功能验证、技术检测；
d) 预置条件：
   1) 被测移动智能终端及预置应用软件处于正常工作状态；
   2) 被测移动智能终端打开测试模式。
e) 测评步骤：
   1) 使用检测工具检测或检查厂商提供的资料性文件，判断其是否使用基于硬件的安全保护方式。
f) 单元判定：如果1）结果均为肯定，则测试项判定为未见异常，否则判定为不符合要求。

8.1.3 个人信息的使用

8.1.3.1 个人信息的安全性控制

8.1.3.1.1 测评项：详见6.3.1

该项测评方法如下：

a) 指标要求：移动智能终端及预置应用软件应对个人信息访问进行安全性控制，保证个人信息的分析处理过程稳定安全地运行在独立资源空间；
b) 测评对象：移动智能终端、预置应用软件；
c) 测评方式：功能验证、技术检测；
d) 预置条件：
   1) 被测移动智能终端及预置应用软件处于正常工作状态；
   2) 被测移动智能终端打开测试模式。
e) 测评步骤：
   1) 使用检测工具监测移动智能终端及预置应用软件，判断其个人信息使用是否稳定安全地运行在独立资源空间。

f） 单元判定：如果1）结果为肯定，则测试项判定为未见异常，否则判定为不符合要求。

8.1.3.2 个人信息的展示限制

8.1.3.2.1 测评项：详见6.3.2

该项测评方法如下：

a） 指标要求：涉及通过界面展示个人信息的（如显示屏幕中的弹框、通知、浮窗等），移动智能终端及预置应用软件应提供对需展示中涉及的敏感个人信息采取屏蔽处理、隐藏通知内容等措施的能力；

b） 测评对象：移动智能终端、预置应用软件；

c） 测评方式：功能验证；

d） 预置条件：被测移动智能终端及预置应用软件处于正常工作状态；

e） 测评步骤：

1） 查看移动智能终端及预置应用软件，判断其是否存在通过界面展示个人信息的行为；

2） 查看移动智能终端及预置应用软件，判断其是否提供在账号登陆、消息通知、短信接收场景对展示中涉及的敏感个人信息采取屏蔽处理、隐藏通知内容等措施的能力。

f） 单元判定：如果1）、2）结果为肯定，则测试项判定为未见异常，否则判定为不符合要求。

8.1.3.3 个性化推荐

8.1.3.3.1 测评项：详见6.3.3a）

该项测评方法如下：

a） 指标要求：移动智能终端及预置应用软件使用个人信息进行个性化推荐时，应在相应的业务功能界面中显著区分个性化推荐服务；

b） 测评对象：移动智能终端、预置应用软件；

c） 测评方式：功能验证；

d） 预置条件：被测移动智能终端及预置应用软件处于正常工作状态；

e） 测评步骤：

1） 查看移动智能终端及预置应用软件，判断其是否存在使用个人信息进行个性化推送的行为；

2） 查看移动智能终端及预置应用软件，判断其是否在终端页面中显著区分个性化推送服务，如标明“个性化展示”或“定推”等字样。

f） 单元判定：如果1）结果为否定，则测试项判定为不适用；如果1）、2）结果均为肯定，则测试项判定为未见异常，否则判定为不符合要求。

8.1.3.3.2 测评项：详见6.3.3b）

该项测评方法如下：

a） 指标要求：移动智能终端及预置应用软件使用个人信息进行个性化推荐时，应提供退出或关闭个性化推荐模式的选项。用户退出或关闭个性化推荐模式时，应及时停止继续收集仅用于个性化推荐相关服务的个人信息；

b） 测评对象：移动智能终端、预置应用软件；

c） 测评方式：功能验证、技术检测；

d） 预置条件：

1） 被测移动智能终端及预置应用软件处于正常工作状态；

2） 被测移动智能终端打开测试模式。

e） 测评步骤：

1） 查看移动智能终端及预置应用软件，判断其是否存在使用用户个人信息进行个性化推送的行为；

2） 查看移动智能终端及预置应用软件，判断其是否提供退出或关闭个性化展示模式的选项。

3） 关闭个性化推荐模式，使用检测工具监测移动智能终端及预置应用软件，判断其是否继续收集仅用于个性化推荐相关服务的个人信息。

f） 单元判定：如果1）结果为否定，则测试项判定为不适用；如果1）、2）、3）结果均为肯定，则测试项判定为未见异常，否则判定为不符合要求。

8.1.3.3.3 测评项：详见6.3.3c）

该项测评方法如下：

a） 指标要求：移动智能终端及预置应用软件提供个性化推荐服务，若涉及向第三方提供个人信息的，应向用户明示并获得用户同意；

b） 测评对象：移动智能终端、预置应用软件；

c） 测评方式：功能验证、技术检测；

d） 预置条件：

1） 被测移动智能终端及预置应用软件处于正常工作状态；

2） 被测移动智能终端打开测试模式。

e） 测评步骤：

1） 查看移动智能终端及预置应用软件，判断其是否存在使用用户个人信息进行个性化推送的行为，且涉及向第三方提供个人信息；

2） 查看移动智能终端及预置应用软件，判断其是否向用户明示并获得用户同意。

f） 单元判定：如果1）结果为否定，则测试项判定为不适用；如果1）、2）结果均为肯定，则测试项判定为未见异常，否则判定为不符合要求。

8.1.3.3.4 测评项：详见6.3.3d）

该项测评方法如下：

a） 指标要求：移动智能终端及预置应用软件提供个性化推荐服务，向个人信息主体提供向个人信息主体提供隐私保护相关投诉和反馈渠道，支持对个性化推荐服务问题的受理；

b） 测评对象：移动智能终端、预置应用软件；

c） 测评方式：功能验证、技术检测；

d） 预置条件：

1） 被测移动智能终端及预置应用软件处于正常工作状态；

2） 被测移动智能终端打开测试模式。

e） 测评步骤：

1） 查看移动智能终端及预置应用软件的个性化推荐服务，判断其是否向个人信息主体提供隐私保护相关投诉和反馈渠道，并支持对个性化推荐服务问题的受理；

f） 单元判定：如果1）结果均为肯定，则测试项判定为未见异常，否则判定为不符合要求。

8.1.4 个人信息的加工

8.1.4.1 测评项：详见6.4a）

该项测评方法如下：

a） 指标要求：移动智能终端及预置应用软件加工个人信息的目的、方式、范围不应超出业务功能的实际需要或合理关联，法律法规另有规定的除外；

b） 测评对象：移动智能终端、预置应用软件；

c） 测评方式：功能验证、技术检测；

d） 预置条件：

1） 被测移动智能终端及预置应用软件处于正常工作状态；

2） 被测移动智能终端打开测试模式。

e） 测评步骤：

1） 使用检测工具监控移动智能终端及预置应用软件，判断其个人信息加工是否超出业务功能的实际需要或合理关联；

f） 单元判定：如果1）结果为否定，则测试项判定为未见异常，否则判定为不符合要求。

8.1.4.2 测评项：详见6.4b）

该项测评方法如下：

a） 指标要求：移动智能终端及预置应用软件直接获取或通过第三方间接获取个人信息，进行加工处理形成新的个人信息并用于其他目的，应告知并再次征得用户的同意；

b） 测评对象：移动智能终端、预置应用软件；

c） 测评方式：功能验证、技术检测；

d） 预置条件：

1） 被测移动智能终端及预置应用软件处于正常工作状态；

2） 被测移动智能终端打开测试模式。

e） 测评步骤：

1） 使用检测工具监控移动智能终端及预置应用软件，判断其是否通过第三方获取个人信息后，进行加工处理形成新的个人信息并用于其他目的；

2） 查看移动智能终端及预置应用软件，判断其是否告知并再次征得用户同意。

f） 单元判定：如果1）、2）结果均为肯定，则测试项判定为未见异常，否则判定为不符合要求。

8.1.4.3 测评项：详见6.4c）

该项测评方法如下：

a） 指标要求：移动智能终端及预置应用软件加工个人信息应保证加工过程可控、加工结果准确及完整，符合加工处理的预期；

b） 测评对象：移动智能终端、预置应用软件；

c） 测评方式：功能验证、技术检测；

d） 预置条件：

1） 被测移动智能终端及预置应用软件处于正常工作状态；

2） 被测移动智能终端打开测试模式。

e） 测评步骤：

1） 使用检测工具监控移动智能终端及预置应用软件，判断其加工个人信息过程是否可控，加工结果是否符合加工处理的预期。

f） 单元判定：如果1）结果为肯定，则测试项判定为未见异常，否则判定为不符合要求。

8.1.5 个人信息的传输

8.1.5.1 测评项：详见6.5a）

该项测评方法如下：

a） 指标要求：移动智能终端及预置应用软件对用户个人信息传输应按照约定目的和用途进行，传输数据之前应对数据接收方进行身份确认和授权；

b） 测评对象：移动智能终端、预置应用软件；

c） 测评方式：功能验证、技术检测；

d） 预置条件：

1） 被测移动智能终端及预置应用软件处于正常工作状态；

2） 被测移动智能终端打开测试模式。

e） 测评步骤：

1） 使用检测工具监控移动智能终端及预置应用软件，判断其进行用户数据传输是否按照约定目的和用途进行；

2） 查看移动智能终端及预置应用软件，判断其是否在传输数据之前对数据接收方进行身份确认授权。

f） 单元判定：如果1）、2）结果均为肯定，则测试项判定为未见异常，否则判定为不符合要求。

8.1.5.2 测评项：详见6.4b）

该项测评方法如下：

a） 指标要求：移动智能终端及预置应用软件通过公共网络传输账户设置、传感采集（个人健康生理信息、运动信息、位置信息等）、金融支付等服务相关的用户个人信息时，应保证数据的完整性和抗抵赖性，同时应采用密文方式传输。若涉及敏感个人信息传输的，应进行加密保护（例如HTTPS）；

b） 测评对象：移动智能终端、预置应用软件；

c） 测评方式：功能验证、技术检测；

d） 预置条件：

1） 被测移动智能终端及预置应用软件处于正常工作状态；

2） 被测移动智能终端打开测试模式。

e） 测评步骤：

1） 使用检测工具监控移动智能终端及预置应用软件，判断其是否通过公共网络传输账户设置类、传感采集类、金融支付类用户个人信息及其他敏感个人信息；

2） 使用检测工具监控移动智能终端及预置应用软件，判断其是否采用数字签名等技术手段保证数据的完整性和抗抵赖性，并采用加密方式传输。

f） 单元判定：如果1）、2）结果均为肯定，则测试项判定为未见异常，否则判定为不符合要求。

8.1.6 个人信息的查询、更正与删除

8.1.6.1 个人信息的查询

8.1.6.1.1 测评项：详见6.6.1

该项测评方法如下：

a） 指标要求：移动智能终端及预置应用软件应向用户提供查询其所持有的关于该用户的个人信息及个人信息所使用于的目的、范围，获得上述个人信息的第三方组织、身份或类型；

b） 测评对象：移动智能终端、预置应用软件；

c） 测评方式：功能验证；

d） 预置条件：被测移动智能终端及预置应用软件处于正常工作状态；

e） 测评步骤：

1） 查看移动智能终端及预置应用软件，判断其是否向用户提供查询个人信息相关内容的方法；

2） 查看移动智能终端及预置应用软件，判断其可查询的信息是否包括所持有的关于该用户的个人信息及个人信息所使用于的目的、范围，获得上述个人信息的第三方组织、身份或类型。

f） 单元判定：如果1）、2）结果均为肯定，则测试项判定为未见异常，否则判定为不符合要求。

8.1.6.2 个人信息的更正

8.1.6.2.1 测评项：详见6.6.2

该项测评方法如下：

a） 指标要求：用户发现其个人信息有错误或不完整的，移动智能终端及预置应用软件应为其提供请求更正或补充信息的方法；

b） 测评对象：移动智能终端、预置应用软件；

c） 测评方式：功能验证；

d） 预置条件：被测移动智能终端及预置应用软件处于正常工作状态；

e） 测评步骤：

1） 查看移动智能终端及预置应用软件，判断其是否向用户提供更正或补充个人信息的方法。

f） 单元判定：如果1）结果为肯定，则测试项判定为未见异常，否则判定为不符合要求。

8.1.6.3 个人信息的删除

8.1.6.3.1 测评项：详见6.6.3a）

该项测评方法如下：

a） 指标要求：移动智能终端及预置应用软件应清楚告知用户，可删除个人信息的方法或途径；

b） 测评对象：移动智能终端、预置应用软件；

c） 测评方式：功能验证；

d） 预置条件：被测移动智能终端及预置应用软件处于正常工作状态；

e） 测评步骤：

1） 查看移动智能终端及预置应用软件，判断其是否向用户提供可删除个人信息的方法或途径。

f） 单元判定：如果1）结果为肯定，则测试项判定为未见异常，否则判定为不符合要求。

8.1.6.3.2 测评项：详见6.6.3b）

该项测评方法如下：

a） 指标要求：移动智能终端及预置应用软件如对用户个人信息有本地存储操作，应提供用户个人信息彻底删除功能；

b） 测评对象：移动智能终端、预置应用软件；

c） 测评方式：功能验证；

d） 预置条件：被测移动智能终端及预置应用软件处于正常工作状态；

e） 测评步骤：

1）查看移动智能终端及预置应用软件，判断其是否向用户提供用户个人信息彻底删除功能。

f） 单元判定：如果1）结果为肯定，则测试项判定为未见异常，否则判定为不符合要求。

8.1.6.3.3 测评项：详见6.6.3c）

该项测评方法如下：

a） 指标要求：移动智能终端及预置应用软件在相应条件下后，应主动删除个人信息；

b） 测评对象：移动智能终端、预置应用软件；

c） 测评方式：功能验证；

d） 预置条件：被测移动智能终端及预置应用软件处于正常工作状态；

e） 测评步骤：

1） 查看移动智能终端及预置应用软件，判断其是否在个人信息处理目的已实现、无法实现或者为实现处理目的不再必要时，停止提供产品或服务或者保存期限已届满，个人撤回同意，违反法律法规或者违反约定处理个人信息，法律法规所规定的其他情形下主动删除个人信息。

f） 单元判定：如果1）结果为肯定，则测试项判定为未见异常，否则判定为不符合要求。

8.1.6.3.4 测评项：详见6.6.3d）

该项测评方法如下：

a） 指标要求：在法律、行政法规规定的保存期限未届满，或者删除个人信息从技术上难以实现的，移动智能终端及预置应用软件应当停止除存储和采取必要的安全保护措施之外的处理；

b） 测评对象：移动智能终端、预置应用软件；

c） 测评方式：功能验证；

d） 预置条件：被测移动智能终端及预置应用软件处于正常工作状态；

e） 测评步骤：

1） 查看移动智能终端及预置应用软件，判断在法律、行政法规规定的保存期限未届满，或者删除个人信息从技术上难以实现的情况下，移动智能终端及预置应用软件是否停止除存储或采取必要的安全保护措施之外的处理。

f） 单元判定：如果1）结果为肯定，则测试项判定为未见异常，否则判定为不符合要求。

8.2 个人信息安全控制测评

8.2.1 个人信息数据访问控制管理

8.2.1.1 个人信息访问控制能力

8.2.1.1.1 测评项：详见7.1.1a）

该项测评方法如下：

a） 指标要求：移动智能终端应提供针对一般个人信息访问控制的功能，用户授予该类个人信息访问控制前，移动智能终端应保证应用软件无法对该类信息进行访问控制；

b） 测评对象：移动智能终端；

c） 测评方式：功能验证、技术检测；

d） 预置条件：

1） 被测移动智能终端处于正常工作状态；

2） 被测移动智能终端打开测试模式。

e） 测评步骤：

1） 查看移动智能终端，判断其是否提供针对一般个人信息访问控制的功能；

2） 查看并用检测工具监测移动智能终端，判断在应用软件获得其所申请的个人信息访问控制能力前，终端是否能确保应用软件无法对相关数据进行访问控制。

f） 单元判定：如果1）、2）结果为肯定，则测试项判定为未见异常，否则判定为不符合要求。

8.2.1.1.2 测评项：详见7.1.1b）

该项测评方法如下：

a） 指标要求：移动智能终端应提供针对敏感个人信息访问控制的功能，提供系统弹窗等功能，用户授予该类个人信息访问控制前，移动智能终端应保证无法对该类信息进行访问控制；

b） 测评对象：移动智能终端；

c） 测评方式：功能验证、技术检测；

d） 预置条件：

1） 被测移动智能终端处于正常工作状态；

2） 被测移动智能终端打开测试模式。

e） 测评步骤：

1） 查看移动智能终端，判断其是否提供针对敏感个人信息访问控制的功能；

2） 查看并用检测工具监测移动智能终端，判断应用软件在申请敏感个人信息访问控制时，是否提供系统弹窗用以向用户明示，且在用户授权之前，是否确保应用软件无法对相关数据进行访问控制。

f） 单元判定：如果1）、2）结果为肯定，则测试项判定为未见异常，否则判定为不符合要求。

8.2.1.2 个人信息访问控制管理机制

8.2.1.2.1 测评项：详见7.1.2a）

该项测评方法如下：

a） 指标要求：移动智能终端应提供访问控制能力显性告知的提示方式，移动智能终端及预置应用软件发起申请个人信息访问控制时，应在用户主动确认同意授予后执行相应操作；

b） 测评对象：移动智能终端、预置应用软件；

c） 测评方式：功能验证、技术检测；

d） 预置条件：

1） 被测移动智能终端及预置应用软件处于正常工作状态；

2） 被测移动智能终端打开测试模式。

e） 测评步骤：

1） 查看移动智能终端，判断其是否提供访问控制能力显性告知的提示方式；

2） 申请个人信息访问控制，查看并用检测工具监测移动智能终端，判断其是否在用户主动确认同意授予后执行相应操作。

f） 单元判定：如果1）、2）结果为肯定，则测试项判定为未见异常，否则判定为不符合要求。

8.2.1.2.2 测评项：详见7.1.2b）

该项测评方法如下：

a） 指标要求：移动智能终端访问控制能力的授予可根据具体场景分为允许、禁止、询问等选项供用户自由选择。移动智能终端操作系统应供安全防护能力，未被授权的应用软件无法获取相关数据或调用相应接口；

b） 测评对象：移动智能终端；

c） 测评方式：功能验证、技术检测；

d） 预置条件：

1） 被测移动智能终端处于正常工作状态；

2） 被测移动智能终端打开测试模式。

e） 测评步骤：

1） 查看移动智能终端，判断其是否提供个人信息访问控制能力授予的选项供用户选择，可根据具体场景为允许、禁止、询问等选项；

2） 查看移动智能终端，判断未被授权的应用软件是否可以获取相关数据或调用相应接口。

f） 单元判定：如果1）结果为肯定，且2）结果为否定，则测试项判定为未见异常，否则判定为不符合要求。

8.2.1.2.3 测评项：详见7.1.2c）

该项测评方法如下：

a) 指标要求：移动智能终端应提供个人信息访问控制能力撤销授予的功能；

b) 测评对象：移动智能终端；

c) 测评方式：功能验证；

d) 预置条件：被测移动智能终端处于正常工作状态；

e) 测评步骤：

1) 查看移动智能终端，判断其是否提供个人信息访问控制能力撤销授予的功能。

f) 单元判定：如果1）结果为肯定，则测试项判定为未见异常，否则判定为不符合要求。

8.2.1.2.4 测评项：详见7.1.2d）

该项测评方法如下：

a) 指标要求：移动智能终端应提供个人信息访问控制能力配置管理的功能；

b) 测评对象：移动智能终端；

c) 测评方式：功能验证；

d) 预置条件：被测移动智能终端处于正常工作状态；

e) 测评步骤：

1) 查看移动智能终端，判断其是否提供个人信息访问控制能力配置管理的功能。

f) 单元判定：如果1）结果为肯定，则测试项判定为未见异常，否则判定为不符合要求。

8.2.1.2.5 测评项：详见7.1.2e）

该项测评方法如下：

a) 指标要求：已授予的个人信息访问控制能力在移动智能终端操作系统或应用软件版本升级前后应保持一致，如出现能力变更等变化情况，应向用户明示并征得用户授权同意；

b) 测评对象：移动智能终端、预置应用软件；

c) 测评方式：功能验证；

d) 预置条件：被测移动智能终端及预置应用软件处于正常工作状态；

e) 测评步骤：

1) 查看移动智能终端或预置应用软件，判断其是否在个人信息访问控制能力变更后，向用户明示并征得用户授权同意。

f) 单元判定：如果1）结果为肯定，则测试项判定为未见异常，否则判定为不符合要求。

8.2.1.3 安全调用控制能力

8.2.1.3.1 测评项：详见7.1.3a）

该测评项符合YD/T 2408—2021中 4.3.1.1 规定的通信类功能受控机制的测试方法。

8.2.1.3.2 测评项：详见7.1.3b）

该测评项符合YD/T 2408—2021中 4.3.1.2 规定的本地敏感行为受控机制的测试方法。

8.2.2 敏感行为管理

8.2.2.1 应用软件行为记录能力要求

8.2.2.1.1 测评项：详见7.2.1a）

该测评项符合YD/T 2408—2021中 4.5.2.1 规定的应用软件调用行为记录能力的测试方法。

8.2.2.1.2 测评项：详见7.2.1b）

该测评项符合YD/T 2408—2021中 4.5.2.2 规定的应用软件调用行为记录能力的测试方法。

8.2.2.1.3 测评项：详见7.2.1c）

该项测评方法如下：

a） 指标要求：移动智能终端应支持并统计自研预置应用软件调用行为；

b） 测评对象：移动智能终端；

c） 测评方式：功能验证；

d） 预置条件：被测移动智能终端处于正常工作状态；

e） 测评步骤：

1） 查看移动智能终端，判断其自研预置应用软件是否存在通过移动通信网络联网，调用定位、拍照/摄像、后台截屏/录屏、通话录音、本地录音、读取短信、读取电话本、读取媒体影音数据（如照片、视频和音频），读取生物特征数据（如指纹识别、人脸识别等）、读取设备唯一可识别信息（主要指不可重置的设备标识符，如IMEI、MAC地址等）的行为；

2） 查看移动智能终端，判断其是否记录并统计预置应用上述调用行为。

f） 单元判定：如果1）、2）结果均为肯定，则测试项判定为未见异常，否则判定为不符合要求。

8.2.2.1.4 测评项：详见7.2.1d）

该项测评方法如下：

a） 指标要求：移动智能终端应支持并统计自研预置应用软件调用行为；

b） 测评对象：移动智能终端；

c） 测评方式：功能验证；

d） 预置条件：被测移动智能终端处于正常工作状态；

e） 测评步骤：

1） 查看移动智能终端，判断其自研预置应用软件是否存在拨打电话、发起三方通话、发送短信、接收短信、发送彩信、读取传感器信息、读取彩信、读取通话记录、读取日程表、读取上网记录、读取应用软件列表、修改短信、修改彩信、修改电话本、修改通话记录、修改日程表、修改上网记录的行为；

2） 查看移动智能终端，判断其是否记录并统计预置应用上述调用行为。

f） 单元判定：如果1）、2）结果均为肯定，则测试项判定为未见异常，否则判定为不符合要求。

8.2.2.2 行为记录安全管理要求

8.2.2.2.1 测评项：详见7.2.2a）

该项测评方法如下：

a) 指标要求：移动智能终端应支持并统计应用软件调用行为，且用户可查看记录；
b) 测评对象：移动智能终端；
c) 测评方式：功能验证；
d) 预置条件：被测移动智能终端处于正常工作状态；
e) 测评步骤：
   1) 查看移动智能终端，判断其是否支持并统计应用软件调用行为，且用户可查看记录；
   2) 查看移动智能终端，判断其记录的调用行为是否准确，调用行为的起始时间是否为应用软件调用相应功能接口的时间；
   3) 查看移动智能终端调用行为记录判断其是否存在记录内容确实、错误现象。
f) 单元判定：如果1）、2）结果均为肯定，且3）结果为否定，则测试项判定为未见异常，否则判定为不符合要求。

8.2.2.2.2 测评项：详见7.2.2b）

该项测评方法如下：

a) 指标要求：移动智能终端操作系统应提供调用行为记录数据保护机制，防止调用行为记录数据库被恶意删改；
b) 测评对象：移动智能终端；
c) 测评方式：功能验证、技术检测；
d) 预置条件：
   1) 被测移动智能终端处于正常工作状态；
   2) 被测移动智能终端打开测试模式。
e) 测评步骤：
   1) 查看移动智能终端，判断其是否提供调用行为记录数据保护机制；
   2) 使用检测工具检测移动智能终端，判断调用行为记录数据库是否能被恶意删改。
f) 单元判定：如果1）结果为肯定，且2）结果为否定，则测试项判定为未见异常，否则判定为不符合要求。

8.2.2.3 应用软件敏感行为状态展示

8.2.2.3.1 测评项：详见7.2.3

该项测评方法如下：

a) 指标要求：移动智能终端应提供应用软件敏感行为状态展示功能，当应用软件存在调用定位服务、麦克风、摄像头等行为时，应通过持续性状态指示等显著方式对用户进行敏感行为展示；
b) 测评对象：移动智能终端；
c) 测评方式：功能验证；
d) 预置条件：被测移动智能终端处于正常工作状态；
e) 测评步骤：
   1) 查看移动智能终端，判断其是否提供应用软件敏感行为状态展示功能；

2） 查看移动智能终端，判断当应用软件调用定位服务、麦克风、摄像头等功能时，移动智能终端是否存在显著方式对敏感行为进行状态展示；

3） 查看移动智能终端调用行为记录判断其是否存在记录内容确实、错误现象。

f） 单元判定：如果1）、2）结果均为肯定，则测试项判定为未见异常；如果2）结果为否定，判定为不符合要求。

8.2.2.4 高风险行为监测

8.2.2.4.1 测评项：详见7.2.4

该项测评方法如下：

a） 指标要求：移动智能终端应提供针对APP静默安装、热更新等高风险行为的监测能力；

b） 测评对象：移动智能终端；

c） 测评方式：功能验证；

d） 预置条件：被测移动智能终端处于正常工作状态；

e） 测评步骤：

1） 查看移动智能终端，判断其是否提供针对APP静默安装、热更新等高风险行为的监测能力包括但不限于未经用户同意私自安装APP、通过热更新的方式非法改变APP功能、APP图标等行为。

f） 单元判定：如果1）结果为肯定，则测试项判定为未见异常；如果1）结果为否定，判定为不符合要求。

8.2.3 匿名设备识别码

8.2.3.1 测评项：详见7.3a）

该项测评方法如下：

a） 指标要求：移动智能终端提供匿名设备识别码，其生成应具备不可逆性，仅由匿名设备识别码无法关联到该设备的其他非匿名设备识别码；

b） 测评对象：移动智能终端；

c） 测评方式：功能验证、技术检测；

d） 预置条件：

1） 被测移动智能终端处于正常工作状态；

2） 被测移动智能终端打开测试模式。

e） 测评步骤：

1） 查看移动智能终端匿名设备识别码，判断其是否具备不可逆性；

f） 单元判定：如果1）结果为肯定，则测试项判定为未见异常，否则判定为不符合要求。

8.2.3.2 测评项：详见7.3b）

该项测评方法如下：

a） 指标要求：移动智能终端提供匿名设备识别码，应向用户提供重置匿名设备识别码的方法；

b） 测评对象：移动智能终端；

c） 测评方式：功能验证；

d） 预置条件：被测移动智能终端处于正常工作状态；

e） 测评步骤：

1） 查看移动智能终端匿名设备识别码，判断其是否向用户提供重置匿名设备识别码的方法。

f） 单元判定：如果1）结果为肯定，则测试项判定为未见异常，否则判定为不符合要求。

8.2.3.3 测评项：详见7.3c）

该项测评方法如下：

a） 指标要求：移动智能终端提供匿名设备识别码，应向用户提供关闭匿名设备识别码的机制，用户关闭后，APP调用时终端不应返回匿名设备识别码，应返回0或返回关闭状态值；

b） 测评对象：移动智能终端；

c） 测评方式：功能验证；

d） 预置条件：被测移动智能终端处于正常工作状态；

e） 测评步骤：

1） 查看移动智能终端匿名设备识别码，判断其是否向用户提供关闭匿名设备识别码的方法；

2） 查看用户关闭后，是否返回0或返回关闭状态值。

f） 单元判定：如果1）、2）结果均为肯定，则测试项判定为未见异常，否则判定为不符合要求。

8.2.4 自启动与关联启动行为管理

8.2.4.1 测评项：详见7.4a）

该项测评方法如下：

a） 指标要求：移动智能终端应提供移动智能终端应用软件自启动、关联启动关闭选项；

b） 测评对象：移动智能终端；

c） 测评方式：功能验证；

d） 预置条件：被测移动智能终端处于正常工作状态；

e） 测评步骤：

1） 查看移动智能终端是否提供移动智能终端应用软件自启动、关联启动关闭的相关功能。

f） 单元判定：如果1）结果为肯定，则测试项判定为未见异常，否则判定为不符合要求。

8.2.4.2 测评项：详见7.4b）

该项测评方法如下：

a） 指标要求：移动智能终端应提供移动智能终端应用软件自启动、关联启动行为记录，包括自启动、关联启动时间、启动次数及关联启动源、目的应用软件等信息；

b） 测评对象：移动智能终端；

c） 测评方式：功能验证；

d） 预置条件：被测移动智能终端处于正常工作状态；

e） 测评步骤：

1） 查看移动智能终端是否提供移动智能终端应用软件自启动、关联启动行为记录，包括自启动、关联启动时间、启动次数及关联启动源、目的应用软件等信息。

f） 单元判定：如果1）结果为肯定，则测试项判定为未见异常，否则判定为不符合要求。

8.2.4.3 测评项：详见7.4c）

该项测评方法如下：

a） 指标要求：移动智能终端应提供应用软件关联启动的实时提示；

b） 测评对象：移动智能终端；

c） 测评方式：功能验证；

d） 预置条件：被测移动智能终端处于正常工作状态；

e） 测评步骤：

1）查看移动智能终端是否提供应用软件关联启动的实时提示功能。

f） 单元判定：如果1）结果为肯定，则测试项判定为未见异常，否则判定为不符合要求。

8.2.5 系统更新安全管理

8.2.5.1 测评项：详见7.5

该测评项符合YD/T 2408—2021中 4.3.2.1规定的操作系统授权更新的测试方法。

8.2.6 APP的下载、安装、使用

8.2.6.1 测评项：详见7.6

该项测评方法如下：

a） 指标要求：移动智能终端预置应用软件不应存在欺骗误导强迫下载、安装、使用APP的行为；

b） 测评对象：移动智能终端、预置应用软件；

c） 测评方式：功能验证；

d） 预置条件：被测移动智能终端处于正常工作状态；

e） 测评步骤：

1） 查看移动智能终端及预置应用软件，判断其是否提供APP下载、安装、使用的功能；

2） 查看移动智能终端及预置应用软件APP下载、安装、使用功能，判断其是否在提供功能前以显著方式向用户明示、并征得用户同意；

3） 查看移动智能终端及预置应用软件，判断其是否存在点击信息窗口任意位置即下载、安装APP的行为；

4） 查看移动智能终端及预置应用软件，判断其是否存在未明示下载APP情况下通过“是否立即开始游戏”、“领取红包”、“手机卡顿”、“耗电太快”、“内存已满”信息诱导用户点击下载安装；

5） 暂停或取消的APP下载、安装服务，判断是否会自动恢复下载、安装；

6） 查看下载后的APP，判断其是否与下载、安装前明示的APP信息不相符。

f） 单元判定：如果1）结果为否定，则判断结果为不适用；如果1）、2）结果均为肯定，且3）、4）、5）、6）结果均为否定，则测试项判定为未见异常，否则判定为不符合要求。

9 个人信息保护能力评估与分级

本标准将移动智能终端所支持的个人信息保护自低到高分为五个能力等级，每一等级定义了个人信息保护能力要求的最小集合，移动智能终端必须支持该集合中的所有能力才能标识为该等级。移动智能终端可选支持到不同的等级。具体的能力划分详见表1。

表 1 移动智能终端个人信息保护能力评级对照表

技术要求		能力等级要求				
		一级	二级	三级	四级	五级
1	6.1.1.1a） 收集个人信息的告知	√	√	√	√	√
2	6.1.1.1b）个人信息处理规则变更时的告知	√	√	√	√	√
3	6.1.1.1c）内容涉及敏感个人信息的突出显示	√	√	√	√	√
4	6.1.1.1d）收集敏感个人信息的告知	—	—	—	—	√
5	6.1.1.1e）收集未成年人信息的告知	√	√	√	√	√
6	6.1.1.2 收集个人信息的同意	√	√	√	√	√
7	6.1.1.3a）收集敏感个人信息的单独同意	√	√	√	√	√
8	6.1.1.3b)不满十四周岁未成年人信息的告知同意	√	√	√	√	√
9	6.1.1.4 基于个人信息访问控制能力的告知与授权	√	√	√	√	√
10	6.1.1.5 操作系统敏感行为的告知和授权	√	√	√	√	√
11	6.1.2 收集个人信息的最小必要	√	√	√	√	√
12	6.1.3 个人信息的主动提供	√	√	√	√	√
13	6.2.1 个人信息的保存期限	√	√	√	√	√
14	6.2.2a)个人信息本地临时文件存储	—	√	√	√	√
15	6.2.2b）个人信息分类分级存储	—	—	√	√	√
16	6.2.2c)用户口令安全存储及安全访问控制	√	√	√	√	√
17	6.2.2d) 基于硬件的安全存储	—	—	—	—	√
18	6.3.1 个人信息的安全性控制	—	√	√	√	√
19	6.3.2 个人信息的展示限制	√	√	√	√	√
20	6.3.3a）个性化推荐标识	√	√	√	√	√

表 1　移动智能终端个人信息保护能力评级对照表（续）

技术要求		能力等级要求				
		一级	二级	三级	四级	五级
21	6.3.3b）个性化推荐退出和关闭	√	√	√	√	√
22	6.3.3c）涉及向第三方提供信息的个性化推荐	√	√	√	√	√
23	6.3.3d）个性化推荐的用户投诉和反馈	√	√	√	√	√
24	6.4 个人信息的加工	√	√	√	√	√
25	6.5a）个人信息传输的身份确认和授权	√	√	√	√	√
26	6.5b）个人信息传输的安全性	—	—	√	√	√
27	6.6.1a） 个人信息的查询	√	√	√	√	√
28	6.6.1b） 个人信息目的、范围的查询	—	—	√	√	√
29	6.6.1c） 第三方获得个人信息的查询	—	—	√	√	√
30	6.6.2 个人信息的更正	√	√	√	√	√
31	6.6.3a）个人信息删除方式的告知	√	√	√	√	√
32	6.6.3b）本地个人信息的彻底删除	√	√	√	√	√
33	6.6.3c）个人信息的主动删除	—	—	√	√	√
34	7.1.1 个人信息访问控制能力	√	√	√	√	√
35	7.1.2 个人信息访问控制管理机制	√	√	√	√	√
36	7.1.3 安全调用控制能力	符合YD/T 2407—2021中7.2规定的分级要求				
37	7.2.1a） 应用软件行为记录—基础要求	√	√	√	√	√
38	7.2.1b） 应用软件行为记录—增强要求	—	—	—	—	√
39	7.2.1a） 自研预置应用软件行为记录—基础要求	—	—	—	√	√
40	7.2.1b） 自研预置应用软件行为记录—增强要求	—	—	—	—	√
41	7.2.2 行为记录安全管理要求	√	√	√	√	√
43	7.2.3 应用软件敏感行为状态展示	√	√	√	√	√
44	7.2.4 高风险行为监测	—	—	—	√	√
45	7.3a） 匿名设备识别码的不可逆性	√	√	√	√	√
46	7.3b）匿名设备识别码的重置	√	√	√	√	√
47	7.3c）匿名设备标识码的关闭	—	—	—	√	√
48	7.4a）自启动与关联启动的关闭	√	√	√	√	√
49	7.4b）自启动与关联启动行为记录	—	—	√	√	√
50	7.4c）关联启动的实时提示	—	—	—	—	√
51	7.5 系统更新的安全受控	√	√	√	√	√

表 1　移动智能终端个人信息保护能力评级对照表（续）

技术要求		能力等级要求				
		一级	二级	三级	四级	五级
52	7.6 APP下载、安装、使用管理	√	√	√	√	√

电信终端产业协会团体标准

移动智能终端个人信息保护规范

T/TAF 161—2023

*

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