ICS 33.050
CCS M 30

团　体　标　准

T/TAF 187—2023

框架型应用软件个人信息保护规范

Specification of personal information protection on frame-based application software

2023-10-31 发布　　2023-10-31 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、北京抖音信息服务有限公司、蚂蚁科技集团股份有限公司、北京快手科技有限公司、阿里巴巴（中国）有限公司、北京三快在线科技有限公司、华为技术有限公司、荣耀终端有限公司、小米通讯技术有限公司、维沃移动通信有限公司、博鼎实华（北京）技术有限公司、中兴通讯股份有限公司、厦门美柚股份有限公司。

本文件主要起草人：王淞鹤、宋恺、刘陶、王艳红、武林娜、王宇晓、桑明臣、周飞、陈鑫爱、李京典、李可心、宁华、钱康、杜蕾、李昳婧、林冠辰、落红卫、王昕、方强、刘瑾、王芳、李实、赵晓娜、李辰淑、顾泽宇、张玮、董雾、张宏伟、黄鹏华。

引　　言

当前移动互联网行业，小程序等轻量级应用快速发展，其中框架型应用软件作为小程序载体平台，对于当前小程序领域中存在的个人信息保护和用户权益等方面的相关问题，承担着重要责任和义务。

因此，本文件根据《个人信息保护法》《电信和互联网用户个人信息保护规定》（工业和信息化部第24号令）《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》（工信部信管[2020]164号）等法律法规及规范性文件要求，对框架型应用软件的个人信息保护及安全能力进行规范，进一步促进移动互联网行业的健康稳定发展。

框架型应用软件个人信息保护规范

1 范围

本文件规定了框架型应用软件安全能力及用户权益保护相关个人信息保护要求。

本文件适用于框架型应用软件规范个人信息保护能力，也适用于主管监管部门、第三方评估机构等组织对相关个人信息保护能力进行监督、管理和评估。

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。

YD/T 4184—2022 移动互联网应用程序（APP）用户权益保护测评规范

T/TAF 180.1—2023 小程序个人信息保护规范 第1部分：申请授权行为

T/TAF 180.2—2023 小程序个人信息保护规范 第2部分：个人信息收集行为

T/TAF 078.2—2020 APP用户权益保护测评规范 定向推送

T/TAF 078.3—2020 APP用户权益保护测评规范 个人信息获取行为

T/TAF 078.5—2020 APP用户权益保护测评规范 违规使用个人信息

T/TAF 078.7—2023 APP用户权益保护测评规范 第7部分：欺骗误导强迫行为

3 术语和定义

YD/T 4184—2022 界定的术语和定义适用于本文件。

3.1

框架型应用软件 frame-based application software

框架型应用软件是指在移动智能终端上，提供数据访问控制和小程序分发等管理能力，并为在其上运行的第三方的小程序提供相应开发接口的应用软件。

3.2

小程序 mini-program

小程序是指在框架型应用软件上运行的，通过框架型应用软件提供的功能接口，实现某项或某几项特定功能的免安装的应用软件。

3.3

个人信息 personal information

以电子或者其他方式记录的与已识别或者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。

3.4

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。

3.5

授权 authorization

框架型应用软件为小程序提供的申请数据或资源的一种方式。范围涵盖框架型应用所存储的数据或资源及其从操作系统中获取到的数据或资源。

4 框架型应用软件安全能力要求

4.1 访问控制管理

4.1.1 访问控制能力要求

框架型应用软件个人信息访问控制能力应满足以下要求：

a) 应对小程序可申请的信息和授权进行安全访问控制；

b) 涉及小程序通过框架型应用软件的开放接口获取个人信息或授权的，在用户对弹窗授权前，框架型应用软件应保证小程序无法对相关数据或资源进行访问及控制；

c) 涉及框架型应用软件向小程序共享个人信息的，框架型应用软件应向用户明示，并获得用户的单独同意。

注1：小程序可申请的信息参见T/TAF 180.2-2023附录A。

注2：小程序可申请的授权参见T/TAF 180.1-2023附录A。

4.1.2 访问控制管理机制要求

框架型应用软件对访问控制能力的申请授予、撤销、升级和配置管理应满足如下要求：

a) 申请授予要求：访问控制能力的申请授予可根据具体场景分为允许、禁止等选项供用户自由选择；

b) 撤销要求：用户可在小程序界面进行访问控制能力的撤销授予操作，可修改为禁止或询问；

c) 配置管理要求：应提供访问控制能力配置管理功能，供用户自主选择（如小程序主体维度或授权维度）。用户可在配置管理界面对小程序的访问控制能力进行授予、撤销等操作；

d) 一致性要求：应保证已授予小程序的个人信息访问控制能力在其版本升级前后保持一致，如出现能力变化导致原有信息范围扩大的，应向用户重新明示并征得用户授权同意。

4.2 敏感行为记录能力

框架型应用软件应支持记录在其上运行的小程序通过关键接口获取个人信息及系统资源的行为。记录结果不少于7日，且可供用户查看。

注：行为记录范围参见T/TAF 180.1-2023附录A及T/TAF 180.2-2023附录A。

5 框架型应用软件用户权益保护要求

框架型应用软件的用户权益保护应满足YD/T 4184-2022中5至12章节的相关要求。

6 框架型应用软件分发平台管理要求

6.1 分发平台信息明示

框架型应用软件应对小程序分发进行信息明示，具体包括以下要求：

a) 框架型应用软件应对在架小程序进行全量公示；
b) 框架型应用软件小程序搜索结果页面或分发页面应显著明示所分发小程序名称、功能、版本号、开发者或运营者信息、授权列表及用途、个人信息处理规则，确保展示样式的一致性，不应根据开发运营者身份、市场地位等因素区别对待；
c) 框架型应用软件小程序搜索结果页面所明示的小程序名称、图标应与用户点击运行的小程序名称、窗口图标一致；
d) 框架型应用软件明示的小程序开发者或运营者信息应与小程序的隐私政策、用户协议或小程序资料页等自声明中的开发者或运营者信息一致。

6.2 小程序开发者审核

框架型应用软件应建立小程序管理制度，具体满足如下要求：

a) 应对所分发的小程序在上架前进行严格审核，登记并留存小程序名称、开发运营主体、已授权列表、个人信息处理规则、上线时间、功能简介等信息，且留存时间不少于 60 日；
b) 所分发小程序的运营者或开发者为非个人开发者时，应对开发者主体进行认证，确保身份真实有效，如通过营业执照、银行账户等方式验证，应保留其组织机构代码、营业执照等信息；
c) 所分发小程序的运营者或开发者为个人开发者时，应对开发者主体进行实名认证，确保身份信息应真实有效；
d) 小程序涉及提供金融、新闻、出版、医疗保健、药品和医疗器械、社交、游戏等互联网信息服务的，框架型应用软件应对小程序开发者或运营者提供的资质证明文档进行形式审核；
e) 对所分发小程序个人信息处理规则进行审核，保证其真实有效；
f) 框架型应用软件根据监管机构的处置要求及时处理违法违规的小程序；
g) 宜对小程序的软件提供者、运营者、开发者提供的服务信息内容、数据资料及其运营行为等的真实性、合法性及有效性进行审核。

6.3 小程序安全要求

框架型应用软件应对小程序进行上架前安全检测和上架后跟踪监测或定期抽测，包括以下要求：

a) 应对小程序通过其所提供接口的方式调用或访问终端系统资源的行为进行上架前审查和上架后监测；
b) 应对小程序进行安全检测，包括隐私窃取、恶意扣费、远程控制、恶意传播、诱骗欺诈、病毒木马等；
c) 应对小程序恶意绕过上架审核修改基本功能等行为进行检测，具体包括小程序擅自更改主要功能、授权范围、个人信息收集使用的场景和范围等；
d) 应对小程序的个人信息收集情况进行上架前审查和上架后监测。

6.4 小程序用户权益要求

框架型应用软件应对小程序用户权益保护情况进行上架前审核和上架后跟踪监测或定期抽测，包含但不限于以下内容：

a) 小程序违规收集、超范围收集个人信息，具体参考 T/TAF 180.2—2023 第 5-8 章节；
b) 小程序违规使用个人信息，具体参考 T/TAF 078.5 第 3 章节；
c) 小程序申请授权行为，具体参考 T/TAF 180.1—2023；
d) 小程序定向推送，具体参考 T/TAF 078.2 第 3 章节；
e) 小程序欺骗误导强迫行为，具体参考 T/TAF 078.7 第 6-8 章节；
f) 小程序欺骗误导用户提供个人信息，具体参考 T/TAF 078.3。

6.5 小程序内容安全要求

框架型应用软件应对小程序内容进行上架前审核和上架后跟踪监测或定期抽测，发现小程序存在下列内容之一或在相关主管部门监督检查中发现的违法违规小程序，应予以及时下架处理：

a) 反对宪法所确定的基本原则的；
b) 危害国家安全，泄露国家秘密，颠覆国家政权，破坏国家统一的；
c) 损害国家荣誉和利益的；
d) 煽动民族仇恨、民族歧视，破坏民族团结的；
e) 破坏国家宗教政策，宣扬邪教和封建迷信的；
f) 散布谣言，扰乱社会秩序，破坏社会稳定的；
g) 散布淫秽、色情、赌博、暴力、凶杀、恐怖或者教唆犯罪的；
h) 侮辱或者诽谤他人，侵害他人合法权益的；
i) 含有法律、行政法规禁止的其他内容的。

6.6 小程序广告要求

小程序上架前，框架型应用软件宜对小程序的广告进行审核，小程序上架后，框架型应用软件应对其进行跟踪监测或定期抽测，发现存在侵害用户权益的应用应及时采取处置措施，包括但不限于：

a) 小程序内广告不应干扰其他应用或设备的功能。广告应仅能在投放该广告的小程序内展示，不应存在霸占屏幕的行为，包括锁屏界面、解锁后的桌面，且小程序退出或关闭后，小程序内广告应同时关闭；
b) 小程序内广告不应存在频繁弹出影响用户使用的行为，如用户每次点击操作均弹出广告，关闭广告后仍弹出广告导致用户需连续关闭广告；
c) 小程序内广告内容应满足 6.5 小程序内容安全要求。

6.7 小程序付费要求

框架型应用软件应对小程序付费功能进行监督管理，具体要求如下：

a) 小程序应遵守明码标价等相关规定，明示收费标准、收费方式，明示内容应真实准确、醒目规范，不应在付费后仍存在其他未明示的使用条件。扣费前需经用户确认，不应存在恶意吸费行为，如：未在商品购买和商品支付界面提供给用户进行二次确认等；
b) 小程序存在自动续订、自动续费功能的，应清晰明示产品功能权益及资费内容，应当征得用户同意，不得默认勾选、强制捆绑开通；
c) 小程序存在自动续订、自动续费功能的，应提供便捷的随时退订的方式和自动续订、自动续费的取消途径；
d) 小程序存在自动续订、自动续费功能的，在自动续订、自动续费前 5 日，需要以短信、消息推送等显著方式提醒用户。

6.8 申诉投诉

框架型应用软件应建立投诉受理流程，具体包括：

a) 提供小程序开发运营者投诉渠道，如客服热线等，及时处理、反馈开发运营者的申诉事项；

b) 提供用户反馈渠道，建立用户投诉、举报及问题处理流程，对用户反馈存在问题的小程序进行验证，如确认存在问题的，应及时采取处理措施。

电信终端产业协会团体标准

框架型应用软件个人信息保护规范

T/TAF 187—2023

*

版权所有 侵权必究

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