ICS 33.050
CCS M 30

团　体　标　准

T/TAF 149—2023

移动应用分发平台 个人信息保护保障能力评估规范

Mobile application distribution platform—
Evaluation specification of personal information protection and guarantee ability

2023-02-08 发布　　2023-02-08 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、维沃移动通信有限公司、泰尔认证中心有限公司、OPPO广东移动通信有限公司、北京快手科技有限公司、南昌黑鲨科技有限公司、荣耀终端有限公司、小米通讯技术有限公司、北京奇虎科技有限公司、蚂蚁科技集团股份有限公司、阿里巴巴（中国）有限公司、北京三星通信技术研究有限公司、华为技术有限公司、上海兆言网络科技有限公司、北京抖音信息服务有限公司、广州视源电子科技股份有限公司、联想（北京）有限公司、北京微梦创科网络技术有限公司、北京三快在线科技有限公司、珠海市魅族科技有限公司。

本文件主要起草人：王嘉义、陈鑫爱、魏凡星、姜慧格、傅山、刘陶、王艳红、杜云、杨萌科、王宇晓、贾科、张玮、宁华、常琳、付艳艳、李越、落红卫、王昕、沈彭军、赵之成、赵晓娜、顾泽宇、杜文博、姚一楠、彭晋、林冠辰、黄天宁、吴越、衣强、李实、张海燕、钱雷、杨骁涵、肖洋、李洁、李汝鑫、刘俊、高龙、王天、刘瑾、祖岩岩、沈玲、毕烽。

引　言

随着《网络安全法》、《个人信息保护法》的落地和实施，个人信息保护已经成为广大人民群众最关心最直接最现实的利益问题之一，《个人信息保护法》中明确规定个人信息处理者应当对其个人信息处理活动负责，并采取必要措施保障所处理的个人信息的安全。移动应用分发平台成为移动应用下载和使用的主要来源，也是各方关注的焦点，更是保障移动互联网用户合法权益、保障用户个人信息的重点。本标准将落实法律法规的要求，提出移动应用分发平台个人信息保护保障能力评估规范，指导行业进行系统性的保障能力建设、规程建设、技术建设，落实个人信息保护工作。

移动应用分发平台　个人信息保护保障能力评估规范

1　范围

本文件规定了移动应用分发平台个人信息保护保障能力评估规范，主要包含对个人信息的全生命周期保障能力和安全能力，保障用户合法权益。

本文件适用于第三方评估机构开展评估工作，同时也适用于个人信息处理者进行自评估。

2　规范性引用文件

本文件没有规范性引用文件。

3　术语和定义

下列术语和定义适用于本文件。

3.1

移动应用分发平台　application software distribution platform

是指通过应用商店、应用市场、网站等方式提供App下载、升级服务的软件服务平台。

3.2

移动应用软件　mobile application

移动智能终端系统之上安装、运行的，向用户提供服务功能的应用软件，包括集成的 SDK 等第三方产品或服务，包含快应用、小程序等多种形态。

3.3

移动应用软件开发者　mobile application software developer

移动应用开发者是指为移动应用提供软件开发、应用部署等服务的主体(单位或个人)。

3.4

个人信息　personal information

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，本文件中数据指个人信息。

注1:个人信息包括姓名、出生日期、身份证件号码、个人生物识别信息、住址、通信通讯联系方式、通信记录和内容、账号密码、财产信息、征信信息、行踪轨迹、住宿信息、健康生理信息、交易信息等。

注2:个人信息控制者通过个人信息或其他信息加工处理后形成的信息，例如用户画像或特征标签，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，属于个人信息。

4 缩略语

下列缩略语适用于本文件。

APP：移动应用软件（Application）

SDK：软件开发工具包（Software Development Kit）

H5：第五代超文本标记语言（HTML5）

5 个人信息保护保障能力评估概述

5.1 评估原则

开展移动应用分发平台个人信息保护保障能力评估应遵循以下原则：

a) 目的性原则：评估目的应明确具体，评估范围应与评估目的相适应。

b) 可用性原则：应确保保障能力措施实施情况可被准确评测，并能和具体评估指标对应进行评估。

c) 全面性原则：评估应当贯穿个人信息全周期，实现对个人信息保护流程的全面控制。

d) 可调性原则：评估方应确保能够根据评估对象及应用场景不同进行调整，以适应多种情况的评估。

6 个人信息保护保障能力评估指标

6.1 保障功能要求

6.1.1 风险识别与防控

风险识别与防控应满足以下要求：

a) 应根据法律法规要求、合同规定和业务运营需要，对所掌握的个人信息进行分类分级管理；

b) 应采取加密、脱敏、去标识化、备份、访问控制、审计等技术或者其他必要措施，防止个人信息的泄露、篡改、损毁、不正当使用等。

6.1.2 访问控制与审计

访问控制与审计应满足以下要求：

a) 开展个人信息处理活动时，应基于分类分级采取安全管理措施，明确相关人员的访问权限，防止非授权访问；

b) 开展个人信息处理活动时，对个人信息的关键操作，如批量修改、拷贝、删除、下载等，应设置内部审批和审计流程，并严格执行；

c) 应按照审批流程授权个人信息接触岗人员，不应出现未授权的信息类型新增；

d) 访问控制应做到职责权限分离、最小化授权和可溯源审计；

e) 应保证个人信息处理的安全性，在整个过程中个人信息不应被第三方无关人员或组织获知，过程数据应进行保护；

f) 对个人信息进行分析处理时，应保证处理系统稳定安全运行，不造成个人信息的损毁、泄露和丢失等。

6.2 保障管理要求

6.2.1 组织

应满足以下组织要求：

a) 处理个人信息达到国家网信部门规定数量的个人信息处理者应任命专门的个人信息保护负责人，负责人应具备以下要求：
   1) 应具有相关管理工作经历和专业知识；
   2) 具有较强独立性，负责人不宜兼任首席运营官、首席执行官等可能有利益冲突的职位；
   3) 应参与个人信息处理活动的重要决策，并直接向公司主要负责人报告。
b) 应明确企业个人信息保护责任人，负责有关个人信息处理活动的重要决策，履行相关职责，并提供资源保障，包括但不限于提供人力、财力、物力保障；
c) 应设立专门的企业级个人信息保护工作机构，明确机构工作职责，机构内宜包括管理决策、政策支持、技术支持等部门或人员；
d) 个人信息保护机构主要负责统筹个人信息安全工作，具体职责可包括：
   1) 制订工作计划并督促落实；
   2) 制订、签发、实施、更新个人信息保护政策和规程；
   3) 建立、维护、更新个人信息清单和授权访问策略；
   4) 组织开展个人信息安全影响分析与风险评估，督促整改；
   5) 组织开展个人信息安全培训；
   6) 组织产品上线前个人信息安全检测；
   7) 组织个人信息安全审计；
   8) 处理、通报、报告个人信息保护相关工作或事件情况；
   9) 组织受理和处置个人信息保护相关投诉、举报。

6.2.2 制度

应满足以下制度要求：

a) 应建立个人信息管理制度体系，包括但不限于安全策略、管理制度、操作规程、记录表单等；
b) 应制订个人信息保护总体方针和安全策略等相关制度文件，文件内容包括但不限于公司个人信息保护工作目标、范围、原则和安全框架等说明；
c) 应制订个人信息管理规范等制度文件，明确对于个人信息保护的指引和要求，突出个人信息接触岗对个人信息日常管理的操作规程和要求；
d) 个人信息管理制度应由个人信息保护负责人或机构制订，明确制订程序和发布方式；
e) 应对相关制度执行情况进行记录，确保实际工作流程正确执行；
f) 个人信息对外披露或共享时，应按照企业个人信息保护机构制订的流程进行审批，审批通过后才可执行；
g) 定期发布包含个人信息保护内容的社会责任报告，接受社会监督。

6.2.3 管理机制

应满足以下管理机制要求：

应建立健全对所分发的应用软件的管理机制：

a) 应对应用软件开展审核，并对 APP 的安全、服务等进行检测；
b) 应对应用软件进行审核和检测，对违法违规软件进行处置；
c) 应建立完善用户举报投诉处置措施；
d) 应建立完善的开发者申诉处理机制；
e) 对于违法违规应用软件，以及在通信主管部门监督检查中发现的恶意应用软件等违法违规软件，应及时予以下架；

f） 对严重违反法律、行政法规处理个人信息的平台内的产品或者服务提供者，停止提供服务；

6.2.4 监督检查配合

应满足以下监督检查配合要求：

a） 应遵循公开、公平、公正的原则，制定平台规则，明确平台内产品或者服务提供者处理个人信息的规范和保护个人信息的义务；
b） 不应抗拒、不配合监督检查工作；
c） 不应冒用监管机构名义提出整改要求或其他违规动作等；
d） 应按要求及时下架违法应用软件，落实下架等处置要求；
e） 不应阻挠开发者或运营者积极整改，例如无正当理由禁止更新、下架待治理 APP 等。

6.2.5 人员管理与考核

应满足以下人员管理与考核要求：

a） 应与个人信息处理岗员工签订保密协议，明确保密要求；
b） 应明确个人信息处理不同岗位安全职责，明确个人信息安全管理考核指标和问责机制，对相关人员特别是重要岗位人员的履职情况进行考核；出现个人信息安全重大事件时，对直接负责的主管人员和其他直接责任人员进行问责；
c） 应定期进行安全培训、考核，确保人员掌握个人信息安全管理相关流程；
d） 应采用最小权限原则设置人员权限和审批流程，对于批量修改、复制、下载个人信息等行为进行严格审核；
e） 对于超权限操作应经个人信息保护负责人或机构授权并存档记录；
f） 人员工作变动时，应及时调整相应信息访问和使用权限；
g） 应与个人信息接触外部人员或外部组织签订保密协议，明确保密要求；
h） 应建立外部人员访问企业安全措施，规定外部人员可访问区域、访问权限、访问内容和操作记录等要求。

6.2.6 事件应急处置

应满足以下事件应急处置要求：

a） 应制订个人信息安全事件应急预案，包括应急处理流程、事件上报流程等；
b） 应建立个人信息安全事件应急响应机制，并根据个人信息安全计划的变化而及时调整，确保个人信息安全事件得到及时有效处置，应急响应机制应包括：
    1） 个人信息安全事件分级；
    2） 启动条件；
    3） 启动所需的资源，如人员、设备、场所、工具、资金等；
    4） 流程、人员安排和操作手册。
c） 应定期举行个人信息应急培训和应急演练，并定期对原应急预案进行重新评估、完善；
d） 应配备应急响应所需的资源，确保应急响应机制能够有效实施；
e） 应制定应急演练计划，按计划或者在应急响应机制发生变化后，组织开展应急演练，检验和完善应急响应机制，提高实战能力；
f） 发生个人信息安全事件时，个人信息处理者应立即启动应急响应机制，采取相应的补救和防范措施，可能造成危害的，应及时以电话、短信、邮件或者信函等方式告知个人信息主体，同时对可能危害国家安全、公共安全、经济安全和社会稳定的应按相关要求向有关部门报告。

7 个人信息保护保障能力评估流程

7.1 总体要求

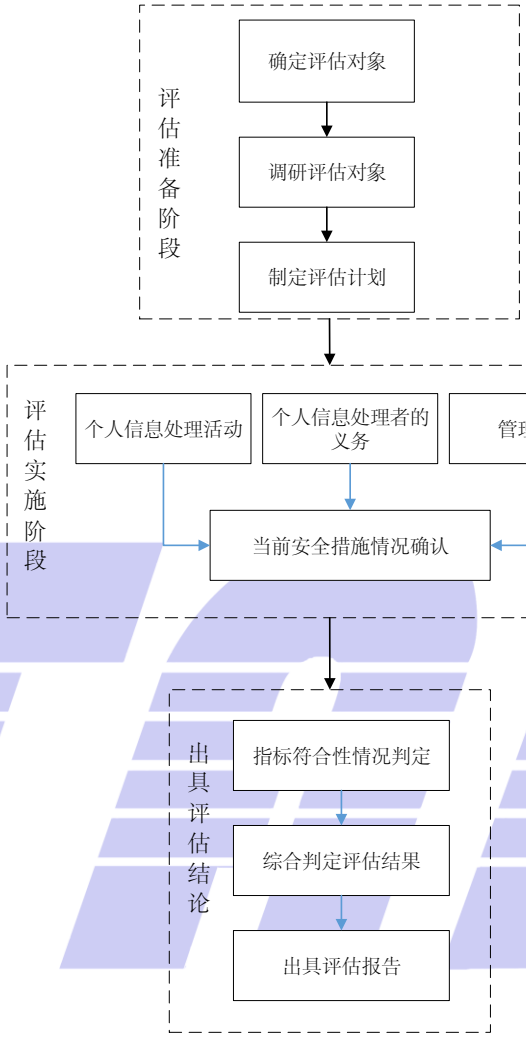

图1 个人信息保护保障能力评估流程图

个人信息保护保障能力评估包括自评估和检查评估两种形式。评估流程分为评估准备、评估实施和出具评估结论三个部分，如图1所示。评估准备阶段应实施以下步骤：

a) 确定评估对象：评估对象可以是被评估方的一种或多种产品或服务，可以是被评估方的某个或多个关键信息系统和关键业务流程，也可以是被评估方的部分或全部系统、部门等；

b) 调研评估对象：评估方应组建相应的评估团队，对评估对象进行充分调研，了解评估对象相关信息，准备相应辅助评估工具等；

c) 制定评估计划：评估方应根据评估对象调研结果制定合理的评估计划安排。

评估实施阶段评估方应根据不同评估内容采用相应的评估方法进行评估，通过问卷、文档审阅和访谈等方法确认评估内容的实际保护措施或要求落实情况等。

出具评估结论阶段应包括评估报告和结论，根据评估实施内容和具体评估指标相符合情况给出说明。

7.2 确定评估对象

根据评估目标，评估方和被评估方应共同确定评估对象。若评估形式为自评估且由评估方自行实施时，应由评估方自行确定评估对象。若评估形式为自评估且由评估方委托第三方实施时，应由评估方和受委托方协商确定，以评估方意见为主，受委托方提供建议。若评估形式为检查评估时，被评估方应配合评估方或评估方委托的第三方确认评估对象。

7.3 调研评估对象

评估对象确认后，应对其相关的保障功能要求和保障管理要求分别进行调研。

保障功能要求应至少包括以下方面：

a) 基本信息管理能力；
b) 主要的业务功能和个人信息处理活动规模；
c) 相关个人信息处理系统；
d) 相关个人信息类型和敏感程度；
e) 相关组织结构和人员；
f) 相关制度和流程。
g) 保障管理要求应至少包括以下方面：
h) 相关组织结构和人员；
i) 相关管理制度和流程。

7.4 制定评估计划

评估方应合理预估评估工作复杂度和工作量，合理制定评估计划。评估计划中应包括以下内容：

a) 评估对象和范围、评估依据、评估环境、评估工具；
b) 评估团队人员角色分工等；
c) 评估工作计划，包括工作内容、输出结果等；
d) 时间进度安排。

7.5 实施评估

应考虑以下方面，实施评估工作：

a) 依据对应的评估规范标准开展实施评估活动；
b) 各部分实施评估工作可顺序开展也可并行开展，无完整的顺序关系；
c) 评估过程中均需输出评估过程文档，其内容至少应包括评估对象、评估所选择的评估指标及针对评估指标的评估结果。

7.6 出具评估结论

应考虑以下方面，给出评估结论：

a) 在评估报告中，应包含评估的环境、评估基本要素和每一项评估的结果，同时还应具体描述评估过程中的步骤，如包含未通过项则评估报告中应包含未通过原因的具体描述；
b) 根据评估对象情况给出整改意见和建议；
c) 若有需要，宜提供整改后复查环节。

8 个人信息保护保障能力评估方法

被评估方通过自证等方式提供证明材料，评估方通过问卷、文档审阅和访谈等方式对证明材料内容进行评估确认。被评估方提供可进行测试的移动应用分发平台版本，评估方通过依据保障功能要求及保障管理要求的评估指标进行确认。

评估方可针对评估条款进行深度分析，并结合市场情况，在量化的基础上制定出量标，按一定的量标实行评估，或采用数学模型方式实行评估。评估方可进行定性评估，结合专家意见征询、民意调查和公识获取综合进行评估。综合上述评估方法，最终出具评估结论。

电信终端产业协会团体标准

移动应用分发平台　个人信息保护保障能力评估规范

T/TAF 149—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