ICS 33.050
M 30

团　体　标　准

T/TAF 077.1-2020

APP 收集使用个人信息最小必要评估规范 总则

Application software user personal information collection and usage minimization and necessity evaluation specification
General principle

2020-11－26 发布　　2020－11－26 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 给出的规则起草。

本文件中的某些内容可能涉及专利。本文件的发布机构不承担识别这些专利的责任。

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、OPPO广东移动通信有限公司、维沃移动通信有限公司、北京奇虎科技有限公司、华为技术有限公司、北京三快在线科技有限公司、小米科技有限责任公司、阿里巴巴(中国)有限公司、北京字节跳动科技有限公司。

本文件主要起草人：王艳红、杜云、宁华、武林娜、胡月、陈鑫爱、周飞、李京典、汤立波、常浩伦、李腾、毛欣怡、贾科、姚一楠、衣强、方强、周圣炎、贾雪飞、杨骁涵、王宇晓、安潇羽。

引　　言

随着移动应用种类和数量呈爆发式增长，APP侵害用户权益事件层出不穷，个人信息保护态势愈加严峻，如何保护用户个人信息，尤其是人脸、通讯录、短信、位置、图片等个人敏感信息受到国家和社会公众高度关注。

APP收集使用个人信息最小必要评估旨在对移动互联网行业收集使用用户人脸、通讯录、短信、位置、图片等个人敏感信息进行规范，落实最小、必要的原则。本系列相关标准：

—T/TAF 077.1-2020 APP 收集使用个人信息最小必要评估规范 总则。

—T/TAF 077.2-2020 APP收集使用个人信息最小必要评估规范 位置信息。

—T/TAF 077.3-2020 APP收集使用个人信息最小必要评估规范 图片信息。

—T/TAF 077.4-2020 APP收集使用个人信息最小必要评估规范 通讯录。

—T/TAF 077.5-2020 APP收集使用个人信息最小必要评估规范 设备信息。

—T/TAF 077.6-2020 APP收集使用个人信息最小必要评估规范 软件列表。

—T/TAF 077.7-2020 APP收集使用个人信息最小必要评估规范 人脸信息。

—T/TAF 077.8-2020 APP收集使用个人信息最小必要评估规范 录像信息。

APP 收集使用个人信息最小必要评估规范 总则

1 范围

本文件明确APP收集使用个人信息最小必要评估规范系列标准中术语定义，规定了收集使用的最小必要原则及要求，是APP收集使用个人信息最小必要评估规范系列标准的引领部分，或为其他移动终端数据相关标准提供参考。

本文件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

下列文件对于本标准的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本标准。凡是不注日期的引用文件，其最新版本（包括所有的修改单）适用于本标准。

GB/T 25069-2010 《信息安全技术 术语》

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 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。

3.1.2

移动应用软件 mobile Application Software

针对智能终端所开发的应用程序，包括智能终端预置应用以及互联网信息服务提供者提供的可以通过智能终端下载、安装、升级、卸载的应用。

注：本标准中规定的移动应用软件（APP）即为个人信息处理者。

3.1.3

个人信息 personal information

个人信息是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。

3.1.4

个人敏感信息 personal sensitive information

敏感个人信息是一旦泄露或者非法使用,可能导致个人受到歧视或者人身、财产安全受到严重危害的个人信息,包括种族、民族、宗教信仰、个人生物特征、医疗健康、金融账户、个人行踪等信息。

3.1.5

个人信息处理 personal information processing

个人信息处理包括个人信息的收集、存储、使用、加工、 传输、提供、公开等活动。

3.1.6

收集 collect

获得个人信息的控制权的行为。

3.1.7

告知同意 inform consent

应用通过弹窗或产品界面等方式提示通知用户收集使用相关权限或信息的的目的、方式、范围等，并获用户做出明确授权的行为。

3.1.8

定向推送 directional Push

基于特定个人信息主体的网络浏览历史、兴趣爱好、消费记录和习惯等个人信息，向该个人信息主体推荐或展示信息内容、提供商品或服务的搜索结果以及推送商业广告等活动。

注：业务实践中，定向推送也被称为个性化展示或个性化推荐。本文件中同时使用定向推送、个性化展示和个性化推荐，具有相同含义。

3.2 缩略语

下列缩略语适用于本文件。

APP 移动应用软件 Application

SDK 软件工具开发包 Software Development Kit

4 最小必要原则

APP进行个人信息处理时应遵循以下最小必要原则，即处理个人信息应当具有明确、合理的目的,并应当限于实现处理目的的最小范围,不得进行与处理目的无关的个人信息处理。

注：当APP提供的业务场景不在“APP收集使用个人信息最小必要评估规范的系列规范”的场景分类内，但业务确有需要时，应满足收集使用个人信息的最小必要原则。

5 个人信息处理最小必要评估要求

5.1 告知同意要求

a) 告知同意应遵循最小必要原则，即APP所提供服务涵盖多项业务功能的，收集使用个人敏感信息时，宜按业务功能进行单项或分项征得用户同意，不宜要求用户一次性接受并授权同意其未申请或使用的业务功能收集个人信息的请求。
b) 告知同意的时机及频率应遵循最小必要原则，宜在收集使用之前或收集使用之际的适当时机告知，增进用户对告知与所收集的个人信息之间关联性的理解；并以必要最小限度的频率告知，确保用户的服务体验质量。

5.2 权限要求

a) 权限的申请应遵循最小必要原则，即只申请与业务功能相关的权限，不应过度申请权限。对于第三方SDK等外部代码的引用，APP应确认其相关权限的申请同样满足最小化原则，限制SDK过度申请权限。如APP的业务场景中，不包含位置相关场景，则不应申请位置权限。
b) APP宜优先采用系统自身功能，代替调用相关敏感权限。在存在替代功能实现方式的情况下，不应以提升用户体验为由，强迫用户授予权限。
c) 权限的使用应遵循最小必要原则，即应合理使用申请的权限，不应滥用权限，且实际使用的权限不应超出告知同意的范围。

5.3 收集要求

a) 收集个人信息的类型应遵循最小必要原则，即在收集个人信息的类型，不应超出业务场景的实际需要，法律法规要求的除外。
b) 收集个人信息的数量应遵循最小必要原则，即在收集个人信息的数量，不应超出业务场景的实际需要。
c) 收集个人信息的频率应遵循最小必要原则，即收集个人信息的频率，不应超出业务场景的实际需要。

5.4 使用要求

a) 使用个人信息的类型、数量及频率应遵循最小必要原则，不应超出业务场景的实际需要，法律法规要求的除外。
b) 使用个人信息时，除目的所必需外，应消除明确身份指向性，避免精确定位到特定个人。
c) 使用个人信息进行定向推送应遵循最小必要原则，即对用户进行用户画像的个人信息不应超出业务场景的实际需要。
d) 使用个人信息进行定向推送应告知用户使用的个人信息来源，是APP收集还是来源于其他第三方。
e) 使用个人信息进行定向推送应显著区分个性化展示和非个性化展示，显著区分的方式包括但不限于：标明“推荐”、“猜你喜欢”等字样，或通过不同的栏目、版块、页面分别展示等。
f) 使用个人信息进行定向推送应当同时向该用户提供关闭个性化展示的选项。此外，APP宜建立用户对个性化展示所依赖的个人信息(如标签、画像维度等)的自主控制机制，保障用户调控定向推送展示相关性程度的能力。

5.5 传输要求

a) 传输个人信息的类型及数量应遵循最小必要原则，不应超出业务场景的实际需要，法律法规要求的除外。
b) 传输个人信息的频率应遵循最小必要原则，不应超出业务场景的实际需要。

5.6 存储要求

a) APP 个人信息的存储包含本地存储和服务器远端存储，均应遵循最小必要原则。
b) 存储个人信息的类型及数量应遵循最小必要原则，不应超出业务场景的实际需要。
c) 存储个人信息的时间应遵循最小必要原则，即存储个人信息的时间，应当为实现处理目的所必要的最短时间，法律法规要求的除外。

5.7 第三方共享要求

个人信息的第三方共享均应遵循最小必要原则，即委托处理、共享、转让、公开披露的个人信息类型、数量及频率，不应超出业务场景的实际需要，法律法规要求的除外。其中，共享个人身份信息、网络身份标识等个人信息前，应征得用户的授权同意。

5.8 删除要求

超出存储期限后，应对个人信息进行删除或匿名化处理。

6 评估流程

APP收集使用个人信息最小必要评估流程如图1所示。包括确定评估目标、选择评估指标、制定评估计划、实施评估及得出评估结论这四个活动。

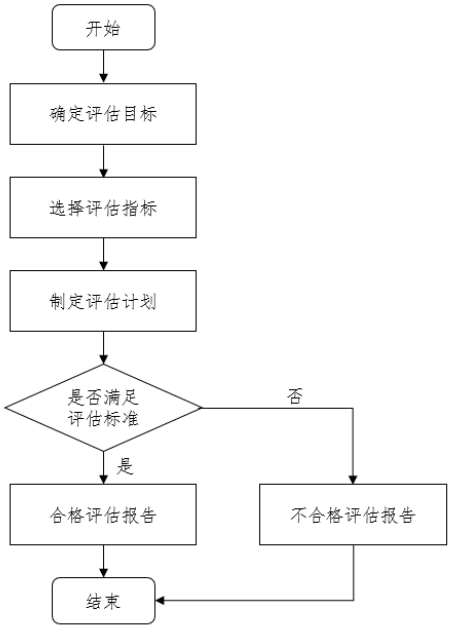

图1 APP收集使用个人信息最小必要评估流程图

6.1 评估方与被评估方

应考虑以下方面，确定评估方和被评估方：
a) 被评估方可为 APP 或者 APP 中某项某类功能。
b) 评估方可为 APP 提供者、开发者和运营者，也可为第三方实验室开展评估参考使用。

6.2 选择评估指标

应考虑以下方面，确定评估指标：

a) 评估方根据被评估方提供的技术说明文档、被评估 APP 样品等材料，确定初步的方案审核，发现涉及的个人信息类型，选择对应的评估规范标准，并由此定义后续的评估的计划和评估项例。

6.3 制定评估计划

应考虑以下方面，制定评估准则：

a) 评估方应根据评估目标，本着公平、公正、公开原则开展评估工作。
b) 评估准则内容应至少包括评估对象和范围、评估依据、评估环境、评估工具。
c) 评估准则中应明确评估通过/不通过准则。

6.4 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) 通过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) 各部分最小必要评估结果均应以评估报告的形式进行输出，其内容至少应包括开展最小必要信息类型、评估所选择的评估指标及针对评估指标的评估结果。

6.5 评估结论

应考虑以下方面，给出评估结论：

a) 针对开展评估的个人信息类别进行评估，APP 收集使用最小必要通过评估并达到目标要求，否则未通过评估。
b) 在最小必要评估报告中，应包含评估的环境、评估基本要素和每一项评估的结果，同时还要具体地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。

电信终端产业协会团体标准

APP 收集使用个人信息最小必要评估规范 总则

T/TAF 077.1-2020

*

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